

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-162600

(43)Date of publication of application : 06.06.2003

(51)Int.Cl.

G06F 17/60

G10K 15/02

H04L 9/08

(21)Application number : 2002-227805

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 05.08.2002

(72)Inventor : NAKAHARA TORU
AZUMA AKIO

(30)Priority

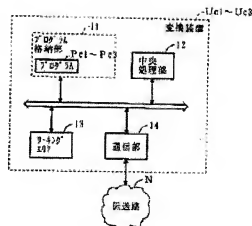
Priority number : 2001241095 Priority date : 08.08.2001 Priority country : JP

(54) LICENSE INFORMATION CONVERSION DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a conversion device Uc1 that converts one's own license information so that it can be transferred to another person.

SOLUTION: Each of at least two terminal devices uses content data according to license information generated in a content delivery system to which each of the devices subscribes. The conversion device Uc1 has a working area 13 in which license information for the terminal device of one side is stored, and a central processing part 12 that converts the license information stored in the working area 13 to the license information for the terminal of other side.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-162600

(P2003-162600A)

(43) 公開日 平成15年6月6日 (2003.6.6)

(51) Int.Cl. ⁷	識別番号	F I	テラトド [*] (参考)
G 0 6 F 17/60	1 4 2	G 0 6 F 17/60	1 4 2 5 J 1 0 4
G 1 0 K 15/02		G 1 0 K 15/02	
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B

審査請求 未請求 請求項の数19 O L (全 27 頁)

- (21) 出願番号 特願2002-227805 (P2002-227805)
- (22) 出願日 平成14年8月5日 (2002.8.5)
- (31) 優先権主張番号 特願2001-241055 (P2001-241055)
- (32) 優先日 平成13年8月8日 (2001.8.8)
- (33) 優先権主張国 日本 (J P)

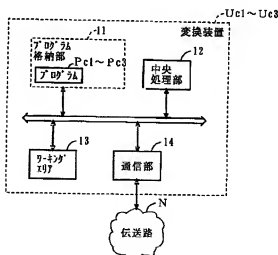
- (71) 出願人 000003821
松下電器産業株式会社
大阪府門真市大字門真1008番地
- (72) 発明者 中原 徹
大阪府門真市大字門真1008番地 松下電器産業株式会社内
- (73) 発明者 東 晋紀男
大阪府門真市大字門真1008番地 松下電器産業株式会社内
- (74) 代理人 100098291
弁理士 小笠原 史朗
Fターム (参考) 5J104 EA15 PA07

(54) 【発明の名称】 ライセンス情報変換装置

(57) 【要約】

【課題】 自分のライセンス情報を、他人に譲渡することが可能なように変換する変換装置Uc1を提供することである。

【解決手段】 少なくとも2台の端末装置はそれぞれ、自身が加入するコンテンツ配信システムで生成されるライセンス情報に従って、コンテンツデータを利用する。変換装置Uc1は、一方の端末装置向けのライセンス情報が格納されるワーキングエリア13と、ワーキングエリア13に格納されたライセンス情報を、他方の端末装置向けのライセンス情報に変換する中央処理部12とを備える。



【特許請求の範囲】

【請求項1】 第1の端末装置向けのライセンス情報を第2の端末装置向けに変換するための変換装置であって、

前記第1および前記第2の端末装置は互いに異なる第1および第2のライセンス情報に従ってコンテンツデータを利用し、

前記変換装置は、

前記第1の端末装置向けの第1のライセンス情報が格納されるワーキングエリアと、

前記ワーキングエリアに格納された第1のライセンス情報を、前記第2の端末装置向けの第2のライセンス情報に変換する処理部とを備える、変換装置。

【請求項2】 前記第1のライセンス情報は、少なくとも、前記コンテンツデータの前記第1の端末装置側での利用を許可するための第1の利用許可情報を含んでおり、

前記処理部は、少なくとも、前記第1のライセンス情報を含む第1の利用許可情報を、前記コンテンツデータの前記第2の端末装置側での利用を許可するための第2の利用許可情報に変換する、請求項1に記載の変換装置。

【請求項3】 前記処理部は、予め定められた変換比率に従って、前記第1のライセンス情報を含む第1の利用許可情報を、前記コンテンツデータの前記第2の端末装置側での利用を許可するための第2の利用許可情報に変換する、請求項2に記載の変換装置。

【請求項4】 前記コンテンツデータは、互いに異なる第1および第2の略号鍵で暗号化された状態で前記第1および第2の端末装置に配信され、

前記第1のライセンス情報はさらに、前記第1の略号鍵で暗号化されたコンテンツデータを復号するための第1の復号鍵を含んでおり、

前記処理部はさらに、前記第1のライセンス情報における第1の復号鍵を、前記第2の略号鍵で暗号化されたコンテンツデータを復号するための第2の復号鍵に置換する、請求項2に記載の変換装置。

【請求項5】 前記第1および第2の端末装置は、第1および第2のサーバと接続されており、

前記第1および第2のサーバは少なくとも、前記第1および第2のライセンス情報を生成して、前記第1および第2の端末装置に送信し、さらに、当該第1および第2のライセンス情報のフォーマットを表す第1および第2のフォーマットデータを保持しており、

前記第1および第2のサーバと通信を行って、前記第1および第2のフォーマットデータを受信する通信部をさらに備え、

前記処理部は、前記通信部が受信した第1および第2のフォーマットデータに従って、前記ワーキングエリアに格納された第1のライセンス情報を、前記第2の端末装置向けの第2のライセンス情報に変換する、請求項1に

記載の変換装置。

【請求項6】 前記第1および第2のライセンス情報のフォーマットを示す第1および第2のフォーマットデータを格納するフォーマット格納部をさらに備え、

前記処理部は、前記フォーマット格納部に格納された第1および第2のフォーマットデータに従って、前記ワーキングエリアに格納された第1のライセンス情報を、前記第2の端末装置向けの第2のライセンス情報に変換する、請求項1に記載の変換装置。

【請求項7】 前記第1の端末装置と通信を行って、当該第1の端末装置が保持する第1のライセンス情報を受信する通信部をさらに備え、前記ワーキングエリアには、前記通信部により受信された第1のライセンス情報が格納される、請求項1に記載の変換装置。

【請求項8】 前記変換装置は、前記第1の端末装置向けの前記第1のライセンス情報を生成する第1のサーバと通信可能に接続されており、

前記変換装置は、前記第1のサーバと通信を行って、当該第1の端末装置向けに生成される第1のライセンス情報を受信する通信部をさらに備え、

前記ワーキングエリアは、前記通信部により受信された第1のライセンス情報を格納する、請求項1に記載の変換装置。

【請求項9】 前記第1の端末装置に組み込まれる、請求項1に記載の変換装置。

【請求項10】 前記処理部は、前記第1および第2の端末装置が正当なユーザか否かを判定し、

前記第1および第2の端末装置の双方が正当なユーザである場合に、前記ワーキングエリアに格納された第1のライセンス情報を、前記第2の端末装置向けの第2のライセンス情報に変換する、請求項1に記載の変換装置。

【請求項11】 前記処理部は、前記第1および第2の端末装置の一方または双方が正当なユーザでない場合、前記ワーキングエリアに格納された第1のライセンス情報を、前記第1の端末装置に送り返す、請求項10に記載の変換装置。

【請求項12】 前記処理部は、前記ワーキングエリアに格納された第1のライセンス情報の構成要素毎に変換処理が許可されているか否かを判定し、

変換処理が許可されていると判断された構成要素のみを使って、前記ワーキングエリアに格納された第1のライセンス情報を前記第2の端末装置向けの第2のライセンス情報に変換する処理部とを備える、請求項1に記載の変換装置。

【請求項13】 前記ライセンス情報は、前記構成要素の変換処理が許可されているか否かを示す変換可否情報

を含んでおり、前記処理部は、前記ワーキングエリアに格納された第1のライセンス情報の構成要素毎に変換処理が許可されているか否かを、第1のライセンス情報に含まれる変換可否情報を使って判定する。請求項12に記載の変換装置。

【請求項14】 前記処理部は、前記ワーキングエリアに格納された第1のライセンス情報の構成要素毎に変換処理が許可されているか否かを示す変換可否情報を、外部から取得し、取得した前記変換可否情報を使って、前記ワーキングエリアに格納された第1のライセンス情報の構成要素毎に変換処理が許可されているか否かを判定する。請求項12に記載の変換装置。

【請求項15】 前記第1の端末装置は、第1のサーバと接続されており、前記処理部は、前記ワーキングエリアに格納された第1のライセンス情報の内、変換処理が許可されていない構成要素を、前記第1のサーバに送り返す。請求項12に記載の変換装置。

【請求項16】 前記処理部は、前記ワーキングエリアに格納された第1のライセンス情報の内、変換処理が許可されていない構成要素を内部に保持する。請求項12に記載の変換装置。

【請求項17】 第1および第2の端末装置が、互いに異なる第1および第2のライセンス情報に従って、コンテンツデータを利用する環境に適用可能な変換方法であって、

前記第1の端末装置向けの第1のライセンス情報をワーキングエリアに格納する格納ステップと、

前記ワーキングエリアに格納された第1のライセンス情報を、前記第2の端末装置向けの第2のライセンス情報に変換する変換ステップとを備える、変換方法。

【請求項18】 コンピュータ装置で実行されるコンピュータプログラムとして実現される、請求項17に記載の変換方法。

【請求項19】 コンピュータ装置で実行されるコンピュータプログラムとして記憶媒体に記録される、請求項17に記載の変換方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、変換装置に関し、より特定的には、端末装置におけるコンテンツデータの利用を制御するライセンス情報を変換する変換装置に関する。

【0002】

【従来の技術】 近年、インターネットに代表されるネットワークのブロードバンド化および常時接続環境により、コンテンツ配信が身近なものになりつつある。このようなコンテンツ配信のさらなる普及には、コンテンツデータに関連する権利（例えば、著作権または販売権）

の保護が重要であることから、従来より様々な権利管理技術の研究および開発がなされている。ここで、本願明細書では、コンテンツデータに関連する権利を、デジタルライツと称する。また、権利管理技術としては、DRM(Digital Rights Management)が代表的である。以下、DRMを組み込んだコンテンツ配信システムについて説明する。

【0003】 従来のコンテンツ配信システムには、サーバと、端末装置とが、ネットワークによりデータ通信可能に接続される。サーバは、コンテンツデータ、コンテンツ復号鍵およびライセンス情報の組みを少なくとも1つ格納している。コンテンツデータは、例えば、音楽を表すデジタルデータであり、予め定められた方式で暗号化される。コンテンツ復号鍵は、暗号化されたコンテンツデータを復号するための鍵である。ライセンス情報は、DRMにおいては、上述のコンテンツデータの利用条件を表す。利用条件としては、コンテンツデータの利用回数が代表的である。

【0004】 以上の構成のコンテンツ配信システムでは、以下のようにして、コンテンツデータは配信される。まず、端末装置は、コンテンツデータの配信をサーバに要求する。コンテンツデータの要求は、一般的に、コンテンツ識別子および端末固有情報を、端末装置がネットワークを介してサーバに送信することで行われる。コンテンツ識別子は、上述のコンテンツデータを一意に特定する情報である。端末固有情報は、端末装置により予め保持されており、上述のコンテンツデータの要求元である端末装置を一意に特定可能な情報である。

【0005】 サーバは、端末装置からの要求に応答して、上述のコンテンツ復号鍵を、今回受信した端末固有情報を使って暗号化する。その後、サーバは、上述の暗号化されたコンテンツデータと、端末固有情報で暗号化されたコンテンツ復号鍵と、ライセンス情報とを端末装置に送信する。端末装置は、サーバにより配信されたコンテンツデータ、コンテンツ復号鍵およびライセンス情報を受信し、内部に備える記憶装置に格納する。

【0006】 以上の格納後、端末装置のユーザは、今回復号されたコンテンツデータを利用可能な状態になる。実際にコンテンツデータを利用する場合、ユーザは、その旨を端末装置に指示する。この指示に応答して、端末装置は、以下のように動作する。端末装置は、記憶装置内のライセンス情報により表される利用条件に、今回の利用が合致しているか否かを判定する。端末装置は、利用条件に合致する場合に限り、以下の処理を実行する。次に、記憶装置内のコンテンツ復号鍵は暗号化されているので、端末装置は、自身が保持する端末固有情報を使って、当該コンテンツ復号鍵を復号する。さらに、記憶装置内のコンテンツデータもまた上述のように暗号化されているので、端末装置は、復号したコンテンツ復号鍵を使って、当該コンテンツデータを復号した後、復号し

たコンテンツデータを再生する。

【0007】

【発明が解決しようとする課題】次に、以上のコンテンツ配信システムが抱えている問題点について説明する。端末装置のユーザ（以下、第1のユーザと称する）は、自分のライセンス情報、つまり、コンテンツデータの利用権を、他のユーザ（以下、第2のユーザと称する）に譲渡したいと思う場合がある。しかしながら、第2のユーザは、上述のコンテンツ配信システムに加入しているとは限らず、別のコンテンツ配信システムに加入している可能性がある。さらに、双方のコンテンツ配信システムの間では、ライセンス情報の構成に差異がある可能性もある。その結果、第2のユーザ側の端末装置は、たとえ、第1のユーザ側の端末装置からライセンス情報を受け取ることができたとしても、受け取ったライセンス情報を解釈することができない。そのため、従来のコンテンツ配信システムでは、自分のライセンス情報を、他人に譲渡することができない。

【0008】また、ユーザは、互いに異なる第1および第2のコンテンツ配信システムに加入しており、第1のコンテンツ配信システムから得たライセンス情報のみを解釈できる第1の端末装置と、第2のコンテンツ配信システムから得たライセンス情報のみを解釈できる第2の端末装置とを持っている場合がある。このような状況では、上述のように、第1および第2のコンテンツ配信システムのそれぞれで使われるライセンス情報の構成に差異がある可能性があるため、第2の端末装置は、第1のコンテンツ配信システムからのライセンス情報を受け取ることができたとしても、それを解釈することができない。そのため、上述の状況下では、ユーザが所有するライセンス情報を、自分の端末装置で利用できない場合が生じてしまう。

【0009】それ故に、本発明の目的は、ライセンス情報で、他人が利用できるように、または他の端末装置で利用できるように変換する変換装置を提供することである。

【0010】

【課題を解決するための手段および発明の効果】上記目的を達成するために、第1の発明は、第1の端末装置向けのライセンス情報を第2の端末装置向けに変換するための変換装置であって、第1および第2の端末装置は互いに異なる第1および第2のライセンス情報に従ってコンテンツデータを利用する。変換装置は、第1の端末装置向けの第1のライセンス情報が格納されるワーキングエリアと、ワーキングエリアに格納された第1のライセンス情報を、第2の端末装置向けの第2のライセンス情報に変換する処理部とを備える。

【0011】第2の発明は第1の発明に従属しており、第1のライセンス情報は、少なくとも、コンテンツデータの第1の端末装置側での利用を許可するための第1の

利用許可情報を含んでいる。また、処理部は、少なくとも、第1のライセンス情報が含む第1の利用許可情報を、コンテンツデータの第3の端末装置側での利用を許可するための第2の利用許可情報に変換する。

【0012】第3の発明は第2の発明に従属しており、処理部は、予め定められた変換比率に従って、第1のライセンス情報が含む第1の利用許可情報を、コンテンツデータの第2の端末装置側での利用を許可するための第2の利用許可情報に変換する。

【0013】第4の発明は、第2の発明に従属しており、コンテンツデータは、互いに異なる第1および第2の暗号鍵で暗号化された状態第1および第2の端末装置に提供される。また、第1のライセンス情報はさらに、第1の暗号鍵で暗号化されたコンテンツデータを復号するための第1の復号鍵を含んでいる。処理部はさらに、第1のライセンス情報における第1の復号鍵を、第2の暗号鍵で暗号化されたコンテンツデータを復号するための第2の復号鍵に置換する。

【0014】以上の第1～第4の発明によれば、変換装置は、第1の端末装置向けの第1のライセンス情報を、第2の端末装置向けの第2のライセンス情報に変換する。これによって、第1のユーザは、自分の第1のライセンス情報を基礎として生成されかつ第2の端末装置で利用可能な第2のライセンス情報を、第2のユーザへと渡すことが可能となる。

【0015】第5の発明は、第1の発明に従属しており、第1および第2の端末装置は、第1および第2のサーバと接続されている。第1および第2のサーバは少なくとも、第1および第2のライセンス情報を生成して、第1および第2の端末装置に送信する。さらに、第1および第2のサーバは、第1および第2のライセンス情報のフォーマットを表す第1および第2のフォーマットデータを保持している。ここで、変換装置は、第1および第2のサーバと通信を行って、第1および第2のフォーマットデータを受信する通信部をさらに備える。また、処理部は、通信部が受信した第1および第2のフォーマットデータに従って、ワーキングエリアに格納された第1のライセンス情報を、第2の端末装置向けの第2のライセンス情報に変換する。

【0016】第6の発明は、第1の発明に従属しており、変換装置はさらに、第1および第2のライセンス情報のフォーマットを示す第1および第2のフォーマットデータを格納するフォーマット格納部を備える。また、処理部は、フォーマット格納部に格納された第1および第2のフォーマットデータに従って、ワーキングエリアに格納された第1のライセンス情報を、第2の端末装置向けの第2のライセンス情報に変換する。

【0017】第7の発明は、第1の発明に従属しており、変換装置はさらに、第1の端末装置と通信を行って、当該第1の端末装置が保持する第1のライセンス情

報を受信する通信部を備える。また、ワーキングエリアには、通信部により受信された第1のライセンス情報が格納される。

【0018】第8の発明は、第1の発明に従属しており、交換装置は、第1の端末装置向けの第1のライセンス情報を生成する第1のサーバと通信可能に接続されている。交換装置は、第1のサーバと通信を行って、当該第1の端末装置向けに生成される第1のライセンス情報を受信する通信部をさらに備える。ワーキングエリアは、通信部により受信された第1のライセンス情報を格納する。

【0019】第9の発明は、第1の発明に従属しており、交換装置は、第1の端末装置に組み込まれる。

【0020】第10の発明は、第1の発明に従属しており、処理部は、第1および第2の端末装置が正当なユーザか否かを判定し、第1および第2の端末装置の双方が正当なユーザである場合に、ワーキングエリアに格納された第1のライセンス情報を、第2の端末装置向けの第2のライセンス情報に変換する。第11の発明は、第10の発明に従属しており、処理部は、第1および第2の端末装置の一方または双方が正当なユーザでない場合、ワーキングエリアに格納された第1のライセンス情報を、第1の端末装置に送り返す。第10および第11の発明によれば、不当なユーザからのライセンス情報の交換処理の要求を排除することができる。

【0021】第12の発明は、第1の発明に従属しており、処理部は、ワーキングエリアに格納された第1のライセンス情報の構成要素毎に変換処理が許可されているか否かを判定し、交換処理が許可されていると判断された構成要素のみを使って、ワーキングエリアに格納された第1のライセンス情報を第2の端末装置向けの第2のライセンス情報に変換する処理部とを備える。

【0022】第13の発明は、第12の発明に従属しており、ライセンス情報は、構成要素の交換処理が許可されているか否かを示す交換可否情報を含んでいる。処理部は、ワーキングエリアに格納された第1のライセンス情報の構成要素毎に変換処理が許可されているか否かを、第1のライセンス情報に含まれる交換可否情報を使って判定する。

【0023】第14の発明は、第12の発明に従属しており、処理部は、ワーキングエリアに格納された第1のライセンス情報の構成要素毎に変換処理が許可されているか否かを示す交換可否情報を、外部から取得し、取得した交換可否情報を使って、ワーキングエリアに格納された第1のライセンス情報の構成要素毎に変換処理が許可されているか否かを判定する。

【0024】第12〜第14の発明によれば、第1のライセンス情報の構成要素毎に、交換処理をコントロールできるので、コンテンツデータの配信者側の意図を考慮した交換装置を提供することができる。

【0025】第15の発明は、第12の発明に従属しており、第1の端末装置は、第1のサーバと接続されており、処理部は、ワーキングエリアに格納された第1のライセンス情報の内、交換処理が許可されていない構成要素を、第1のサーバに送り返す。

【0026】第16の発明は、第12の発明に従属しており、処理部は、ワーキングエリアに格納された第1のライセンス情報の内、交換処理が許可されていない構成要素を内部に保持する。

【0027】第15および第16の発明によれば、交換処理が許可されていない第1のライセンス情報の構成要素については、第1のサーバに返したり、内部に保持したりするので、典型的には、交換後の第2のライセンス情報を、第1のライセンス情報に再変換する際に使うことが可能となる。

【0028】第17の発明は、第1および第2の端末装置が、互いに異なる第1および第2のライセンス情報に従って、コンテンツデータを利用する環境に適用可能な交換方法であって、第1の端末装置向けの第1のライセンス情報をワーキングエリアに格納する格納ステップと、ワーキングエリアに格納された第1のライセンス情報を、第2の端末装置向けの第2のライセンス情報に変換する交換ステップとを備える。

【0029】第18の発明は、第17の発明に従属しており、交換方法は、コンピュータ装置で実行されるコンピュータプログラムとして実現される。第19の発明は、第17の発明に従属しており、交換装置は、コンピュータ装置で実行されるコンピュータプログラムとして記憶媒体に記録される。

【0030】

【発明の実施の形態】「第1の実施形態」図1は、本発明の第1の実施形態に係る交換装置Uc1と、その周辺環境とを示すブロック図である。図1において、交換装置Uc1は、コンテンツ配信システムScd1およびScd2と、有線または無線の伝送路Lnを介して、データ通信可能に接続される。また、コンテンツ配信システムScd1には、少なくとも1つのサーバ21と、少なくとも1つの端末装置22とが、上述の伝送路Lnを介してデータ通信可能に接続される。ここで、サーバ21は、コンテンツ配信の一例としての音楽配信に関わる事業者α側に設置され、端末装置22は、事業者αとの契約に基づいて、音楽配信を受ける契約者β側に設置される。また、コンテンツ配信システムScd2には、少なくとも1つのサーバ31と、少なくとも1つの端末装置32とが、上述の伝送路Lnを介してデータ通信可能に接続される。ここで、サーバ31は、コンテンツ配信の一例としての音楽配信に関わる事業者α側に設置され、端末装置32は、事業者αとの契約に基づいて、音楽配信を受ける契約者β側に設置される。ここで、本実施形態は説明を分かりやすくする観点から、事業者αは事業者αとは異

なる者であり、さらに、契約者 δ は契約者 θ とは異なる者であると仮定する。ただし、契約者 θ は契約者 δ と同一人であっても良い。つまり、契約者 θ でありかつ契約者 δ でもある単一のユーザが、互いに異なるコンテンツ配信システムSed1およびSed2の双方に加入しており、端末装置22および端末装置32の双方を所有している場合にも、本実施形態に係る変換装置Uc1は有効である。

【0031】以下、コンテンツ配信システムSed1およびSed2ならびに変換装置Uc1の順番で、それぞれの詳細な構成について説明する。

【0032】図2は、図1に示すサーバ21および端末装置22の詳細な構成を示すブロック図である。図2において、サーバ21は、コンテンツデータベース（以下、コンテンツDBと称す）211と、復号鍵データベース（以下、復号鍵DBと称す）212と、ユーザ情報データベース（以下、ユーザ情報DBと称す）213と、利用権データベース（以下、利用権DBと称す）214と、中央処理部215と、ワーキングエリア216と、通信部217と、フォーマット格納部218とを備えている。また、端末装置22は、識別子格納部221と、通信部222と、中央処理部223と、ワーキングエリア224と、蓄積装置225とを備えている。

【0033】次に、コンテンツ配信システムSed1において、契約者 θ が事業者 α からコンテンツ配信を受けるまでに必要となる準備について説明する。まず、図2のコンテンツDB211と、復号鍵DB212と、ユーザ情報DB213とが事業者 α により構築される。

【0034】より具体的には、事業者 α は、図3(a)に示すように、契約者 θ に提供すべきコンテンツデータDct1を用意する。コンテンツデータDct1は、端末装置22で利用可能であり、本実施形態では、音楽を表す。また、コンテンツデータDct1のそれぞれに、事業者 α は、コンテンツ識別子Ict1を割り当てる。コンテンツ識別子Ict1は、コンテンツデータDct1の内容を一意に特定するコードである。上述のように、コンテンツデータDct1が音楽を表す場合、コンテンツ識別子Ict1として適用可能なものに、ISRC(International Standard Recording Code)がある。ISRCに関しては、2001年7月23日時点で、<http://www.ifpi.org/index.html>に記載されている。

【0035】さらに、事業者 α は、各コンテンツデータDct1に暗号鍵Kelを割り当てる。専用の暗号鍵Kelにより、以上のコンテンツデータDct1は暗号化され、それによって、暗号済みコンテンツデータDec1が生成される。コンテンツDB211は、図3(b)に示すように、以上のコンテンツ識別子Ict1および暗号済みコンテンツデータDec1の組み合わせの集まりとなる。コンテンツDB211において、コンテンツ識別子Ict1は特に、同じ組みの暗号済みコンテンツデータDec1を一

意に特定する。なお、以下の説明の便宜のため、図3

(a)に示す1つの暗号済みコンテンツデータDec1には、コンテンツ識別子Ict1としての「a」が付加されると仮定する。さらに、その暗号済みコンテンツデータDec1は、暗号鍵Kelとしての「b」により暗号化されると仮定する。

【0036】また、サーバ21から端末装置22には、上述の暗号済みコンテンツデータDec1が配信される。それ故、端末装置22には、暗号済みコンテンツデータDec1を復号可能な復号鍵Kd1が提供される必要がある。そのため、事業者 α は、コンテンツDB211内の各暗号鍵Kel(図4(a)参照)に対応する復号鍵Kd1を準備する。ここで、復号鍵Kd1は、暗号鍵Kelと同じビット列からなっているとしてもよい(共通鍵暗号化方式)、当該暗号鍵Kelと異なるビット列からなっているとしてもよい(公開鍵暗号化方式)。復号鍵DB212は、図4(a)に示すように、前述のコンテンツ識別子Ict1および復号鍵Kd1の組み合わせの集まりとなる。復号鍵DB212において、復号鍵Kd1は、同じ組みのコンテンツ識別子Ict1で特定可能な暗号済みコンテンツデータDec1の復号に使用される。

【0037】なお、以下の説明の便宜のため、図4(a)において、コンテンツ識別子Ict1としての「a」と同じ組みには、復号鍵Kd1として「c」が登録されると仮定する。上述からも明らかであるが、復号鍵Kd1としての「c」は、暗号鍵Kelとしての「b」に対応している。

【0038】また、上述の契約者 θ は、事業者 α から音楽配信を受けるための加入契約を交わす。加入契約に基づいて、事業者 α は、契約者 θ に、端末識別子1tn1を割り当てる。端末識別子1tn1は、コンテンツ配信システムSed1において、契約者 θ の端末装置22を一意に特定する。ユーザ情報DB213は、図4(b)に示すように、以上のような端末識別子1tn1の集まりとなる。ここで図2を再度参照する。以上の端末識別子1tn1はさらに、契約者 θ 側の端末装置22における識別子格納部221にも設定される。

【0039】なお、端末識別子1tn1は、端末装置22の工場出荷時に予め、識別子格納部221に設定されている。このような場合、契約者 θ は、上述の加入契約の際に、端末装置22に設定されている端末識別子1tn1を事業者 α に通知する。事業者 α は、通知された端末識別子1tn1を、上述のユーザ情報DB213に登録する。

【0040】なお、以下の説明の便宜のため、図4(b)に示すように、ユーザ情報DB213には、端末装置22のために、1つの端末識別子1tn1として「x1」が登録されると仮定する。この仮定下では、図2に示すように、識別子格納部221には、端末識別子1tn1としての「x1」が設定される。

【0041】また、図5には、利用権DB214が示されているが、これについては後で説明する。

【0042】図6は、図1のサーバ31および端末装置32の詳細な構成を示すブロック図である。図6において、サーバ31は、コンテンツデータベース（以下、コンテンツDBと称す）311と、復号鍵データベース（以下、復号鍵DBと称す）312と、ユーザ情報データベース（以下、ユーザ情報DBと称す）313と、利用権データベース（以下、利用権DBと称す）314と、中央処理部315と、ワーキングエリア316と、通信部317と、フォーマット格納部318とを備えている。また、端末装置32は、識別子格納部321と、通信部322と、中央処理部323と、ワーキングエリア324と、蓄積装置325とを備えている。

【0043】以上の構成のコンテンツ配信システムScd2においても、コンテンツ配信システムScd1と同様に、まず、コンテンツDB311と、復号鍵DB312と、ユーザ情報DB313とが事業者αにより構築される。

【0044】より具体的には、図3(a)を参照して説明したのと同様に、事業者αは、契約者αに提供すべきコンテンツデータDct2（図示せず）を用意する。ここで、コンテンツデータDct2は、本実施形態では、端末装置32で利用可能であり、音楽を表す。また、コンテンツデータDct2のそれそれには、前述のISRCのように、その内容を一意に特定するコンテンツ識別子Ict2（図7(a)参照）が割り当てられる。ここで、注意を要するのは、事業者αおよびαは、独自にコンテンツデータDct1およびDct2を用意するが、これらは互いに同じ内容を表す場合がある。その一例を挙げると、コンテンツデータDct1およびDct2の双方が同一歌手による同一曲を表す場合である。つまり、本実施形態では、コンテンツデータDct2は、それが表す内容について、コンテンツデータDct1と同一性を有する。このような同一性を有するコンテンツデータDct1およびDct2には、互いに同じコードを有するコンテンツ識別子Ict1およびIct2が割り当てられる。

【0045】さらに、各コンテンツデータDct2には暗号鍵Ke2（図7(a)参照）が割り当てられる。専用の暗号鍵Ke2により、以上のコンテンツデータDct2は暗号化され、それによって、暗号済みコンテンツデータDec2（図7(a)参照）が生成される。ここで、本実施形態では、コンテンツ配信システムScd1およびScd2において、暗号鍵Ke2は、前述の暗号鍵Ke1と同じと仮定する。

【0046】コンテンツDB311は、図7(a)に示すように、コンテンツ識別子Ict2および、暗号済みコンテンツデータDct2の組み合わせの集まりとなる。ここで注意を要するのは、以上のコンテンツDB311において、少なくとも1つの暗号済みコンテンツデータD

ct2は、コンテンツDB211の暗号済みコンテンツデータDct1と、前述の同一性を有する。したがって、このような同一性を有する暗号済みコンテンツデータDec2には、対応する暗号済みコンテンツデータDct1に付加されるコンテンツ識別子Ict1と同一のコードを有するコンテンツ識別子Ict2が付加される。

【0047】なお、説明の便宜のため、図7(a)に示す1つの暗号済みコンテンツデータDec2は、暗号鍵Ke1と同一の暗号鍵Ke2としての「b」で暗号化され、図3(b)の上欄に示す暗号済みコンテンツデータDct1と同一性を有すると仮定する。この仮定下では、上記暗号済みコンテンツデータDec2には、自身と同一性がある暗号済みコンテンツデータDct1のコンテンツ識別子Ict1と同じコードを示す「a」が、コンテンツ識別子Ict2として付加される。

【0048】事業者αの場合と同様の理由で、事業者αは、コンテンツDB311内の各暗号鍵Ke2に対応する復号鍵Kd2を準備する。ここで、復号鍵Kd2は、暗号鍵Ke2と同じビット列からなっているというより（共通暗号化方式）、当該暗号鍵Ke2と異なるビット列からなっているという（公開鍵暗号化方式）。なお、本実施形態では、便宜上、復号鍵Kd2は、前述の暗号鍵Ke1と同一であると仮定する。復号鍵DB312は、図7(b)に示すように、前述のコンテンツ識別子Ict2および、復号鍵Kd2の組み合わせの集まりとなる。

【0049】なお、説明の便宜のため、図7(b)において、コンテンツ識別子Ict2としての「a」と同じ組みには、復号鍵Kd2として「c」が登録されると仮定する。上述からも明らかであるが、復号鍵Kd2としての「c」は、暗号鍵Ke2としての「b」による暗号済みコンテンツデータDct2の復号に使用される。

【0050】また、上述の契約者αもまた、事業者αから音楽配信を受けるための加入契約を交わす。従って、事業者αは、契約者αに、端末識別子Itn2を契約者αに割り当てるか、当該契約者αから受け取るか。端末識別子Itn2は、コンテンツ配信システムScd2において、契約者αの端末装置32を一意に特定する。ユーザ情報DB313は、図8(a)に示すように、以上のような端末識別子Itn2の集まりとなる。また、以上の端末識別子Itn2はさらに、図6に示すように、端末装置32の識別子格納部321にも設定される。

【0051】なお、説明の便宜のため、図8(a)に示すように、ユーザ情報DB313には、1つの端末識別子Itn2として「x2」が登録されると仮定する。この仮定下では、図6に示すように、識別子格納部321には、端末識別子Itn2としての「x2」が設定される。

【0052】また、図8(b)には、利用権DB314が示されているが、これについては後で説明する。

【0053】図9は、図1に示す変換装置Uc1の構成を示すブロック図である。図9において、変換装置Uc1

は、プログラム格納部11と、中央処理部12と、ワーキングエリア13と、通信部14とを備えている。プログラム格納部11は、典型的には、ROMまたはハードディスクドライブで構成され、プログラムPclを格納する。中央処理部12は、プログラムPclに従って動作して、本実施形態の特徴であるライセンス情報の変換処理(図17および図18参照)を行う。ワーキングエリア13は、中央処理部12が各種処理を行う際に使用される。通信部14は、前述の伝送路Nに接続されており、コンテンツ配信システムScd1およびScd2との通信を行う。

【0054】次に、以上のような構成を有する変換装置Uc1、ならびにコンテンツ配信システムScd1およびScd2における動作を説明する。

【0055】以下、まず、図10を参照して、コンテンツ配信システムScd1において、端末装置22がサーバ21からコンテンツ配信を受ける時の各部の処理について説明する。まず、契約者βは、端末装置22を操作して、サーバ21にアクセスして、コンテンツDB211に蓄積されているコンテンツデータDet1の中から、今回取得したいもののコンテンツ識別子Ict1を特定する。以降の説明において、今回特定されたコンテンツデータDet1を、取得対象コンテンツデータDet1と称する。さらに、契約者βは、取得対象コンテンツデータDet1を利用する際の利用条件Cct1を指定する。

【0056】以下、利用条件Cct1について、より詳細に説明する。コンテンツデータDet1が音楽を表す場合、利用条件Cct1としては、有効期間、再生回数、最大連続再生時間、総再生時間または再生品質が代表的である。また、利用条件Cct1は、有効期間、再生回数、最大連続再生時間、総再生時間および再生品質の内、2つ以上の組み合わせであってもよい。利用条件Cct1としての有効期間は、例えば、2001年6月1日から2001年8月31日までと設定され、設定された期間に限り、端末装置22は、コンテンツデータDet1を再生できる。再生回数は、例えば、5回と設定され、設定された回数に限り、端末装置22は、コンテンツデータDet1を再生できる。最大連続再生時間は、例えば、10秒と設定され、端末装置22における1回の再生において、コンテンツデータDet1の再生が許される最大の時間である。このような最大連続再生時間は、音楽のプログラムに特に有効である。総再生時間は、例えば、10時間と設定され、設定された時間の範囲内であれば、端末装置22は、コンテンツデータDet1を自由に再生できる。再生品質は、例えば、CD(Compact Disc)の品質と設定され、端末装置22は、設定された再生品質でコンテンツデータDet1を再生できる。なお、利用条件Cct1の種類は本実施形態の本質的な事項ではないので、当該実施形態では、便宜上、利用条件Cct1は、コンテンツデータDet1の再生回数であるとして、以下

の説明を続ける。

【0057】上述したように、契約者βは、端末装置22を操作して、コンテンツ識別子Ict1および利用条件Cct1を指定する。このような指定により、端末装置22のワーキングエリア224上に、コンテンツ識別子Ict1および利用条件Cct1が格納される。これらの格納に応答して、中央処理部223は、図11(a)に示す取得要求Drrを生成する(図10;ステップS11)。取得要求Drrは、取得対象コンテンツデータDet1の配信をサーバ11に要求するための情報である。ステップS11をより具体的に説明すると、まず、中央処理部223は、識別子格納部221内の端末識別子Itn1をワーキングエリア224に転送する。その後、中央処理部223は、ワーキングエリア224上の端末識別子Itn1、コンテンツ識別子Ict1および利用条件Cct1に、予め定められた取得要求識別子Irrを付加して、取得要求Drr(図11(a)参照)を生成する。ここで、取得要求識別子Irrは、サーバ21が取得要求Drrを特定するために使用される。

【0058】中央処理部223は、生成した取得要求Drrを、ワーキングエリア224から通信部222に転送し、通信部222は、受け取った取得要求Drrを、伝送路Nを通じて、サーバ21に送信する(ステップS12)。

【0059】サーバ21(図2参照)において、通信部217は、伝送路Nからの取得要求Drrを受信して、ワーキングエリア216に転送して格納する。この格納に際して、中央処理部215は、取得要求Drrに設定されている端末識別子Itn1に一致するものが、上述のユーザ情報DB213(図4(b)参照)に登録されているか否かを確認する(ステップS13)。一致する端末識別子Itn1が登録されていない場合、中央処理部215は、今回取得要求Drrが、契約者β以外のものとであると判断して、これを廃棄し(ステップS14)、処理を終了する。また、そうでない場合、中央処理部215は、契約者βの取得要求Drrを受け取ったと判断して、利用権登録処理を行う(ステップS15)。

【0060】ステップS15において、まず、中央処理部215は、まず、その取得要求識別子Irrを確認して、今回、取得要求Drrを受け取ったことを認識する。次に、中央処理部215は、今回の取得要求Drrから、端末識別子Itn1、コンテンツ識別子Ict1、および利用条件Cct1を取り出して、それらの組み合わせを利用権DB214に登録する。ここで、取得要求Drrにより、端末装置22は、コンテンツデータDet1の取得だけでなく、取得対象コンテンツデータDet1の利用権も要求している。つまり、端末識別子Itn1、コンテンツ識別子Ict1および利用条件Cct1の組み合わせは、取得対象コンテンツデータDet1を端末装置22が利用条件Cct1に従って利用するという権利を示す。以上の観

点から、中央処理部215は、取得要求Drrから取り出した組み合わせを利用権情報Drgt1として扱う。つまり、利用権DB214は、図5に示すように、端末識別子Itn1、コンテンツ識別子Ict1および利用条件Cct1で構成される利用権情報Drgt1の組み合わせの集まりとなる。

【0061】ここで、以上の利用権DB214に登録される利用権情報Drgt1の具体例について説明する。既に説明している通り、本実施形態では、利用条件Cct1は再生回数であると仮定されている。さらに、今回の取得要求Drrには、端末識別子Itn1として「x1」、コンテンツ識別子Ict1として「a」および利用条件Cct1として「再生m回」（mは自然数）が設定されていると仮定する。以上の仮定下では、図5に示すように、1つの利用権情報Drgt1には、端末識別子Itn1としての「x1」、コンテンツ識別子Ict1としての「a」および利用条件Cct1としての「再生m回」が設定される。

【0062】なお、本実施形態の技術的特徴とは関係ないが、ステップS15において、中央処理部215は、利用権情報Drgt1の登録毎に、契約者Bに対する課金を行っている。

【0063】次に、中央処理部215は、コンテンツDB211（図3（b）参照）にアクセスして、今回の取得要求Drrにより指定されるコンテンツ識別子Ict1、およびそれが割り当てられている暗号済みコンテンツデータDct1を、図11（b）に示すようなデータセットDst1として、ワーキングエリア216上に読み出す（ステップS16）。中央処理部215は、読み出したデータセットDst1をワーキングエリア216から通信部217に転送し、通信部217は、受け取ったデータセットDst1を、伝送路Nを通じて、端末装置22に送信する（ステップS17）。

【0064】端末装置22において、通信部222は、伝送路NからのデータセットDst1を受信して（ステップS18）、ワーキングエリア224に転送し格納する。この格納に際して、中央処理部223は、それに含まれるコンテンツ識別子Ict1から、今回、送信した暗号済みコンテンツデータDct1を受信したことを認識する。その後、中央処理部223は、コンテンツ識別子Ict1および暗号済みコンテンツデータDct1を、蓄積装置225に格納する（ステップS19）。

【0065】デジタルライツの保護の観点から、端末装置22は、暗号済みコンテンツデータDct1を受信するので、それを利用するには、サーバ21により提供される復号鍵Kd1で、暗号済みコンテンツデータDct1を復号する必要がある。ここで、本コンテンツ配信システムSed1では、復号鍵Kd1を端末装置22に提供するために、後で詳説するライセンス情報Dlc1が用いられる。以下、図12および図13を参照して、端末装置22がサーバ21からライセンス情報Dlc1の提供を受ける時の

各部の処理について説明する。

【0066】まず、契約者Bは、端末装置22を操作して、蓄積装置225に格納されている暗号済みコンテンツデータDct1の中から、今回利用したいものを、復号対象コンテンツデータDct1として指定する。このような指定により、蓄積装置225からワーキングエリア224に、復号対象コンテンツデータDct1およびそのコンテンツ識別子Ict1が転送され格納される（図2；ステップS21）。これらの格納に際して、中央処理部223は、図14（a）に示す発行要求Dirを生成する（ステップS22）。発行要求Dirは、ライセンス情報Dlc1の提供をサーバ21に要求するため、つまり復号対象コンテンツデータDct1の利用許可を受けるための情報である。より具体的にステップS22を説明すると、まず、中央処理部223は、識別子格納部221内の端末識別子Itn1をワーキングエリア224に転送する。その後、中央処理部223は、ワーキングエリア224上の端末識別子Itn1およびコンテンツ識別子Ict1に、予め定められた発行要求識別子Iirを付加して、発行要求Dir（図14（a）参照）を生成する。ここで、発行要求識別子Iirは、サーバ21が発行要求Dirを特定するために使用される。

【0067】中央処理部223は、生成した発行要求Dirを、ワーキングエリア224から通信部222に転送し、通信部222は、受け取った発行要求Dirを、伝送路Nを通じて、サーバ21に送信する（ステップS23）。

【0068】サーバ21（図2参照）において、通信部217は、伝送路Nからの発行要求Dirを受信して、ワーキングエリア216に転送し格納する。この格納に際して、中央処理部215は、発行要求Dirに対して、図10のステップS13と同様の処理を行い（ステップS24）、対象となる端末識別子Itn1がなければ、前述のステップS14と同様に、今回の発行要求Dirを廃棄する（ステップS25）。逆に、対象となる端末識別子Itn1があれば、中央処理部215は、まず、その発行要求識別子Iirを確認して、今回、発行要求Dirを受け取ったことを認識する。

【0069】このように認識すると、中央処理部215は、利用権DB214（図5参照）に、今回の発行要求Dir内のものと同じ端末識別子Itn1およびコンテンツ識別子Ict1を含む利用権情報Drgt1が登録されているか否かを判断する（ステップS26）。

【0070】以上のような利用権情報Drgt1が未登録であれば、中央処理部215は、復号対象コンテンツデータDct1の利用拒否を示す情報である利用拒否を生成して、通信部217および伝送路Nを介して、端末装置22に送信する（ステップS27）。端末装置22において、中央処理部223は、通信部222を通じて、利用拒否を受け取る（ステップS28）。しかし、これに

降、中央処理部223は、復号対象コンテンツデータDect1の復号に必要な処理を行わない。以上のように、本コンテンツ配信システムScd1では、利用権DB214に利用権情報Drgt1が未登録の場合には、サーバ21が端末装置22側での復号を拒否する。これによって、前述のデジタルライツを保護することが可能となる。

【0071】逆に、ステップS26において、利用権情報Drgt1が登録済みであれば、中央処理部215は、それに含まれる利用条件Cct1を参照して、端末装置22に利用許可を与えることができるかを否かを判断する(ステップS29)。利用許可を付与不可能であれば、中央処理部215は、上述のステップS27を実行する。その結果、端末装置22側では、復号対象コンテンツデータDect1の復号に関連する処理が行われない。以上のように、本コンテンツ配信システムScd1では、利用権DB214に有効な利用権情報Drgt1が未登録の場合にも、サーバ21は端末装置22における復号を拒否するので、上述と同様に、デジタルライツを保護することが可能となる。

【0072】逆に、ステップS29において、利用許可を付与可能であれば、中央処理部215は、利用許可情報Dlwlを生成して、ワーキングエリア216に格納する(ステップS210)。利用許可情報Dlwlは、今回の発行要求Dirにより特定される端末装置22にコンテンツデータDct1の利用を許可するための情報である。ただし、端末装置22に無条件で利用許可を付与すると、前述のデジタルライツを保護する観点から好ましくないで、利用許可情報Dlwlは、どのような条件で端末装置22に利用許可を与えるかを示すことが好ましい。ここで、前述したように、利用権情報Drgt1の利用条件Cct1は、端末装置22がコンテンツデータDct1をどのような条件で利用するかを示す。以上の観点から、本実施形態において、利用許可情報Dlwlは、利用条件Cct1を超えない範囲で、端末装置22の利用許可を示すことがさらに好ましい。

【0073】また、本実施形態では、利用許可情報Dlwlの生成により、端末装置22の利用権情報Drgt1の一部または全てが使用される。そのため、ステップS210の次に、中央処理部215は、使用された利用権情報Drgt1を更新する(ステップS211)。

【0074】ここで、以上のステップS26からS211の処理の具体例について説明する。今、利用権DB214には、図5に示すように、端末識別子Itnlとしての「x1」、コンテンツ識別子Ict1としての「a」および利用条件Cct1としての「再生m回」から構成される利用権情報Drgt1が登録されていると仮定する。また、今回の発行要求Dirは、端末識別子Itnlとしての「x1」およびコンテンツ識別子Ict1としての「a」を含んでいると仮定する。

【0075】以上の仮定下では、ステップS26におい

て、端末識別子Itnlとしての「x1」およびコンテンツ識別子Ict1としての「a」を含む利用権情報Drgt1が登録済みであると判断される。さらに、ステップS29において、この利用権情報Drgt1には、「再生m回」と設定されているので、端末装置22に利用許可を与えることが可能と判断される。以上のように判断されると、ステップS210において、利用許可情報Dlwlが生成される。この時生成される利用許可情報Dlwlは、例えば、「再生n回」を示す。ここで、nは、上述のmを超えない自然数であり、より好ましくは、端末装置22の処理能力に応じて設定される。例えば、端末装置22が相対的に低い性能のハードウェアを搭載している場合であれば、nは、「1」のように、端末装置22が復号対象コンテンツデータDect1を利用可能な最低限の値に設定されることが好ましい。また、便宜上、本実施形態では、n=1であるとして、説明を続ける。

【0076】以上のことから、端末装置22(端末識別子Itnlが「x1」)は、コンテンツデータDct1(コンテンツ識別子Ict1が「a」)の利用権をn回使うことになる。そのため、ステップS211において、利用条件Cct1が「再生m回」から「再生(m-n)回」に更新される。

【0077】ステップS211の次に、中央処理部215は、復号鍵DB212(図4(a)参照)から、今回の発行要求Dirに含まれるものと同じコンテンツ識別子Ict1と同じ組みの復号鍵Kdlを、ワーキングエリア216に読み出す(図13;ステップS212)。次に、中央処理部215は、今回の発行要求Dirから、端末識別子Itnlおよびコンテンツ識別子Ict1をワーキングエリア216に取り出す(ステップS213)。以上のステップS213により、ワーキングエリア216上には、端末識別子Itnl、コンテンツ識別子Ict1、利用許可情報Dlwlおよび復号鍵Kdlが揃う。中央処理部215は、次に、ワーキングエリア216上の端末識別子Itnl、コンテンツ識別子Ict1、利用許可情報Dlwlおよび復号鍵Kdlを順番に並べて、図14(b)に示すライセンス情報Dlclを生成する(ステップS214)。以上のライセンス情報Dlclは、復号対象コンテンツデータDect1の端末装置22における利用を制御するための情報である。なお、図14(b)におけるp1~p4については後述する。

【0078】ここで、前述の仮定に従えば、今回のライセンス情報Dlclにおいて、端末識別子Itnlは「x1」であり、コンテンツ識別子Ict1は「a」であり、利用許可情報Dlwlは「1」であり、さらに、復号鍵Kdlは「c」である。

【0079】以上のようにして生成したライセンス情報Dlclを、中央処理部215は、ワーキングエリア216から通信部217に転送し、通信部217は、受け取ったライセンス情報Dlclを、伝送路Nを通じて、端末

装置22に送信する(ステップS215)。なお、ライセンス情報D1c1は、契約者βに無関係な者に利用されてはならないので、サーバ21および端末装置22は、SSL(Secure Socket Layer)に代表される安全な通信下で、ライセンス情報D1c1を交換することが好ましい。

【0080】端末装置22において、通信部222は、伝送路Nからのライセンス情報D1c1を受信して、受信ライセンス情報D1c1に基づいて、それが自局宛のものか否かを判定する(ステップS216)。受信ライセンス情報D1c1が自局宛のものでなければ、中央処理部223は、以降の処理を行わない。それに対して、自局宛のライセンス情報D1c1を受信したと判定した場合、中央処理部223は、それをワーキングエリア224に転送し格納する。この格納に応答して、中央処理部223は、今回のライセンス情報D1c1内の利用許可情報D1w1を参照して、復号対象コンテンツデータDct1の利用許可が付与されているか否かを判定する(ステップS217)。

【0081】利用許可が付与されていなければ、中央処理部223は、以降の処理を行わない。以上のように、本コンテンツ配信システムScd1では、サーバ21から利用許可が付与されない限り、端末装置22は、復号対象コンテンツデータDct1の復号を行えない。これによって、前述のデジタルライツを保護することが可能となる。

【0082】逆に、ステップS217において、利用許可が付与されていれば、中央処理部223は、受け取ったライセンス情報D1c1から、復号鍵Kd1を取り出す(ステップS218)。ここで、以上のステップS217およびS218の具体例について説明する。上述の仮定下では、今回のライセンス情報D1c1の利用許可情報D1w1により、コンテンツデータDct1の再生が1回だけ許可されている。かかる場合、中央処理部223は、利用許可情報D1w1に設定される再生回数が「1」であるから、ステップS217において復号対象コンテンツデータDct1の利用許可が付与されていると判断して、ステップS218において、受け取ったライセンス情報D1c1から復号鍵Kd1としての「c」を取り出す。

【0083】次に、前述したように、ワーキングエリア224には、復号対象コンテンツデータDct1がすでに格納されている(図12:ステップS21参照)。この復号対象コンテンツデータDct1を得ることが可能となり、図示しないスピーカから音楽を出力させる。これにより、契約者βは、好みの音楽を聴くことができる。なお、中央処理部223は、本実施形態のように、利用許可情報D1w1が再生回数を示す場合には、以上のコンテ

ンツデータDct1の再生が終了する度に、今回のライセンス情報D1c1における利用許可情報D1w1を「1」だけデクリメントすることが好ましい。

【0084】また、図6に示すコンテンツ配信システムScd2においても、コンテンツ配信システムScd1と同様に、端末装置32は、サーバ31からコンテンツ配信およびライセンス情報の提供を受ける。コンテンツ配信時の両者の処理は、図10を参照すれば明らかであり、ライセンス情報提供時の両者の処理は、図12および図13を参照すれば明らかであるため、その説明を省略する。また、ライセンス情報提供時、サーバ31は、図8(b)に示す利用権DB314を参照して、ライセンス情報D1c1と同様に、端末装置32における、コンテンツデータDct2の利用を制御するためのライセンス情報D1c2を生成する。

【0085】なお、以上の説明において、コンテンツデータDct1は、音楽を表すだけに限らず、端末装置22が利用可能であれば、どのようなデータであってよい。その例として、テレビ番組、映画、ラジオ番組、音楽、書籍または印刷物等、コンテンツデータDct1は表している。また、以上の説明では、コンテンツデータDct1が音楽を表す場合の利用条件Cct1について説明した。しかし、上述のみに限らず、利用条件Cct1は、コンテンツデータDct1が表す内容に応じて、適切に設定されることが好ましい。以上の説明では、便宜上、コンテンツデータDct1が音楽を表すことから、端末装置22は、ステップS218で復号されたコンテンツデータDct1が表す音楽をスピーカから出力するとして説明した。しかし、これに限らず、端末装置22は、コンテンツデータDct1の種類に応じて、テレビ番組、映画、書籍および印刷物およびゲーム内容を映像出力可能なもの、ラジオ番組を音声出力可能なものに置換されてもよい。さらに、端末装置22は、復号されたコンテンツデータDct1を、外部の機器(テレビジョン受像機、ラジオ受信機、音楽再生機、電子ブックリーダー、ゲーム機器、PC、情報携帯端末、携帯電話、外部記憶装置等)に転送可能なインターフェイスを備えている。以上のことは、コンテンツ配信システムScd2にも同様当てはまる。

【0086】ところで、上述の説明では、端末装置22は、サーバ21から提供されたライセンス情報D1c1を使って、コンテンツデータDct1の利用を制御するようにしていた。それに加えて、契約者βは、自分のライセンス情報D1c1を、コンテンツデータDct1の利用のために使わず、事業者αのコンテンツ配信に加入している契約者δに譲渡したい場合がある。しかしながら、従来、ライセンス情報D1c1の譲渡は、コンテンツ配信システムScd1およびScd2が色々な面でポリシーが互いに異なる事業者αおよびβにより管理されるので、困難であった。また、契約者βは契約者δと同一人である場

合、ユーザは、コンテンツ配信システムScd1で利用可能なライセンス情報D1c1を、コンテンツ配信システムScd2に対応する端末装置32で使いい場合もある。しかしながら、従来、このようなライセンス情報D1c1の変更もまた、事業者 α および β の互いに異なるポリシーに起因して困難であった。

【0087】ここで、本実施形態では、事業者 α および β のポリシーの相違が、ライセンス情報D1c1およびD1c2のフォーマットに現れていると仮定する。ここで、ライセンス情報D1c1は、図14(b)を参照して説明したが、より具体的には、端末識別子1tn1は、ライセンス情報D1c1の先頭ビットから起算して、p1ビットまでに、コンテンツ識別子1ct1は、(p1+1)ビットからp2ビットまでに、利用許可情報D1w1は、(p2+1)ビットからp3ビットまでに、さらに、復号鍵Kd1は、(p3+1)ビットからp4ビットまでに設定される。ここで、p1~p4は、p1<p2<p3<p4を満たす自然数である。

【0088】以上のライセンス情報D1c1のフォーマットを表すフォーマットデータDfn1が、サーバ21のフォーマット格納部218に格納される。前述のように、ライセンス情報D1c1は、端末識別子1tn1、コンテンツ識別子1ct1、利用許可情報D1w1および復号鍵Kd1という構成要素から構成される。この場合、フォーマットデータDfn1は、図15(a)に示すように、ライセンス情報D1c1の構成要素に相当する4組の要素情報Int11およびビット位置情報1bp11~要素情報Int14およびビット位置情報1bp14から構成される。要素情報Int11は、端末識別子1tn1を特定する。要素情報Int12は、コンテンツ識別子1ct1を特定する。要素情報Int13は、利用許可情報D1w1を特定する。さらに、要素情報Int14は、復号鍵Kd1を特定する。また、ビット位置情報1bp11は、端末識別子1tn1の開始ビット位置である1およびその終了ビット位置であるp1から構成される。ビット位置情報1bp12は、コンテンツ識別子1ct1の開始ビット位置である(p1+1)およびその終了ビット位置であるp2から構成される。ビット位置情報1bp13は、利用許可情報D1w1の開始ビット位置である(p2+1)および終了ビット位置であるp3から構成される。また、ビット位置情報1bp14は、復号鍵Kd1の開始ビット位置である(p3+1)および終了ビット位置であるp4から構成される。

【0089】また、ライセンス情報D1c2は、上述のようにサーバ32で生成される情報であり、図15(b)に示すように、端末識別子1tn2、コンテンツ識別子1ct2、利用許可情報D1w2および復号鍵Kd2を含んでいる。ここで、利用許可情報D1w2は、端末装置32におけるコンテンツデータDct2の利用を制御するための情報である。端末識別子1tn2は、ライセンス情報D1c2の先頭ビットから起算して、q1ビットまでに、コンテ

ンツ識別子1ct2は、(q1+1)ビットからq2ビットまでに、利用許可情報D1w2は、(q2+1)ビットからq3ビットまでに、さらに、復号鍵Kd2は、(q3+1)ビットからq4ビットまでに設定される。ここで、q1~q4は、q1<q2<q3<q4を満たす自然数である。

【0090】ここで、注意を要するのは、前述したように、ライセンス情報D1c1は、コンテンツ識別子1ct1により特定されるコンテンツデータDct1の利用を制御する情報である。従って、ライセンス情報D1c2において、コンテンツ識別子1ct2は、ライセンス情報D1c1により利用可能なコンテンツデータDct1と同一性を有するコンテンツデータDct2のものでなくてはならない。また、本実施形態では、互いに同一性があるコンテンツデータDct1およびDct2には、同じコードのコンテンツ識別子1ct1および1ct2が割り当てられる。以上のことから、上述のp1およびq1は同じ値であるとして、以降の説明を続ける。また、前述したように、本実施形態では、復号鍵Kd1およびKd2は互いに同じであると仮定されている。以上のことから、(p3-p2)および(q3-q2)は同じ値として、以降の説明を続ける。つまり、本実施形態では、端末識別子1tn1および端末識別子1tn2を表現するためのビット数と、利用許可情報D1w1およびD1w2を表現するためのビット数とが相違する。

【0091】以上のライセンス情報D1c2のフォーマットを表すフォーマットデータDfn2が、サーバ31のフォーマット格納部318に格納される。フォーマットデータDfn2は、図16に示すように、ライセンス情報D1c2の構成要素に関連して、4組の要素情報Int21およびビット位置情報1bp21~要素情報Int24およびビット位置情報1bp24から構成される。要素情報Int21は、端末識別子1tn2を特定する。要素情報Int22は、コンテンツ識別子1ct2を特定する。要素情報Int23は、利用許可情報D1w2を特定する。さらに、要素情報Int24は、復号鍵Kd2を特定する。また、ビット位置情報1bp21は、端末識別子1tn2の開始ビット位置である1およびその終了ビット位置q1から構成される。ビット位置情報1bp22は、コンテンツ識別子1ct2の開始ビット位置である(q1+1)およびその終了ビット位置q2から構成される。ビット位置情報1bp23は、利用許可情報D1w2の開始ビット位置(q2+1)および終了ビット位置q3から構成される。また、ビット位置情報1bp24は、復号鍵Kd2の開始ビット位置(q3+1)および終了ビット位置q4から構成される。

【0092】上述のように、契約者 β 側の端末装置32は、ライセンス情報D1c2を解釈することはできるが、ライセンス情報D1c1をそのまま受け取っても、解釈することができないという問題点があった。そこで、変換装置Uc1は、ライセンスの変換処理を行って、ライセン

ス情報D1c1のフォーマットを、端末装置32で利用できるように変換する。

【0093】以下、図17および図18を参照して、ライセンス交換時における変換装置Uc1および端末装置22の処理について説明する。まず、契約者βは、端末装置22を操作して、今回交換対象となるライセンス情報D1c1を指定する。さらに、契約者βは、端末装置22を操作して、交換対象となるライセンス情報D1c1を最終的に利用する端末識別子Itn2を指定する。さらに、契約者βは、端末装置22を操作して、変換元のライセンス情報D1c1が使用可能なコンテンツ配信システムScd1と、フォーマット変換先のコンテンツ配信システムScd2とを指定する。このような指定により、ワーキングエリア224上に、ライセンス情報D1c1と、端末識別子Itn2と、変換元特定情報Iciおよび交換先特定情報Idi(図19(a)参照)が格納される。ここで、変換元特定情報Iciとは、コンテンツ配信システムScd1のサーバ21を特定する情報であり、交換先特定情報Idiとは、コンテンツ配信システムScd2のサーバ31を特定する情報である。

【0094】以上の格納に応答して、中央処理部223は、図19(a)に示すような交換要求Dcrを、ワーキングエリア224上で生成する(図17;ステップS31)。交換要求Dcrは、上述のライセンス情報D1c1の交換を交換装置Uc1に要求するための情報であり、図19(a)に示すように、端末識別子Itn2と、上述の変換元特定情報Iciおよび交換先特定情報Idiとを含んでいる。

【0095】中央処理部223は、生成した交換要求Dcrおよびライセンス情報D1c1を、ワーキングエリア224から通信部222に転送し、通信部222は、受け取った交換要求Dcrおよびライセンス情報D1c1を、伝送路Nを通じて、交換装置Uc1に送信する(ステップS32)。なお、ライセンス情報D1c1は、契約者βに無関係な者に利用されてはならないので、交換装置Uc1および端末装置22は、SSL(Secure Socket Layer)に代表される安全な通信下で、少なくともライセンス情報D1c1を交換することが好ましい。

【0096】交換装置Uc1(図9参照)において、通信部14は、伝送路Nからの交換要求Dcrおよびライセンス情報D1c1を受信して、ワーキングエリア13に転送し格納する(ステップS33)。この格納に際して、中央処理部12は、プログラム格納部11内のプログラムPc1に従って動作し、まず、今回の交換要求Dcrから、端末識別子Itn2、変換元特定情報Iciおよび交換先特定情報Idiを取り出す(ステップS34)。その後、中央処理部12は、図19(b)および(c)に示すような、交換可否要求Dcq1およびDcq2を、ワーキングエリア13上で生成する(ステップS35)。こ

こで、交換可否要求Dcq1は、交換対象となるライセンス情報D1c1を送ってきた端末装置22がコンテンツ配信システムScd1の正当な契約者βであるか否かを示す第1の交換可否情報Iack1の送信をサーバ21に要求するための情報であり、図19(b)に示すように、少なくとも端末装置22の端末識別子Itn1および変換元特定情報Iciとを含んでいる。ここで、注意を要求するのは、交換装置Uc1は、端末装置22と安全な通信のためにコネクションを確立しているので、交換要求Dcrに端末識別子Itn1を設定せずとも、端末識別子Itn1を取得できる点である。また、交換可否要求Dcq2は、交換後のライセンス情報D1c2を使う端末装置32がコンテンツ配信システムScd2の正当な契約者βであるか否かを示す第1の交換可否情報Iack2の送信をサーバ32に要求するための情報であり、図19(c)に示すように、少なくとも端末装置32の端末識別子Itn2および交換先特定情報Idiを含んでいる。

【0097】中央処理部12は、生成した交換可否要求Dcq1およびDcq2を、ワーキングエリア13から通信部14に転送し、通信部14は、受け取った交換可否要求Dcq1およびDcr2を、伝送路Nを通じて、サーバ21および31に送信する(ステップS36)。

【0098】サーバ21および31(図10および図6参照)において、通信部217および317は、伝送路Nからの交換可否要求Dcq1およびDcq2を受信して、ワーキングエリア216および316に転送し格納する(ステップS37)。格納された交換可否要求Dcq1およびDcq2を解釈した後、中央処理部215および315は、それぞれに設定される端末識別子Itn1およびItn2が、コンテンツ配信システムScd1およびScd2のユーザリスト(図示せず)に登録されているか否かをチェックする(ステップS38)。

【0099】その後、中央処理部215および315の双方は、ステップS38のチェック結果に従って、図19(d)および(e)に示すような、第1の交換可否情報Iack1およびIack2をワーキングエリア216および316上で作成する(ステップS39)。第1の交換可否情報Iack1は、サーバ21によるステップS38のチェック結果、つまり、端末装置22がコンテンツ配信システムScd1の正当なユーザか否かを示す情報を含んでいる。また、第1の交換可否情報Iack2は、端末装置32がコンテンツ配信システムScd2の正当なユーザか否かを示す情報を含んでいる。

【0100】中央処理部215および315は、生成した第1の交換可否情報Iack1およびIack2を、ワーキングエリア216および316から通信部217および317に転送し、通信部217および317は、受け取った第1の交換可否情報Iack1およびIack2を、伝送路Nを通じて、交換装置Uc1に送信する(ステップS310)。

【0101】交換装置Uc1(図9参照)において、通信

部14は、伝送路Nからの第1の変換可否情報Iack1およびIack2を受信して、ワーキングエリア13に格納する(ステップS311)。その後、中央処理部12は、格納された第1の変換可否情報Iack1およびIack2を解釈して、端末装置22および32がコンテンツ配信システムScd1およびScd2の正当なユーザーであるか否かを判定する(ステップS312)。

【0102】中央処理部12は、端末装置22および23のいずれか一方で正当なユーザーでないと判断した場合、今回のライセンス情報Dlc1を端末装置22に送り返し(ステップS313)。その後、図17および図18の処理は終了する。それに対して、ステップS312で、端末装置22および23の双方が正当なユーザーであると判断された場合には、中央処理部12は、図19(f)および(g)に示すような、フォーマット送信要求Dfr1およびDfr2を、ワーキングエリア13上で生成する(図18;ステップS314)。ここで、フォーマット送信要求Dfr1およびDfr2は、交換元特定情報Iciおよび交換先特定情報Dldで特定されるサーバ21および31にフォーマットデータDfm1およびDfm2の送信を要求するための情報である。

【0103】中央処理部12は、生成したフォーマット送信要求Dfm1およびDfm2を、ワーキングエリア13から通信部14に転送し、通信部14は、受け取ったフォーマット送信要求Dfr1およびDfr2を、伝送路Nを通じて、サーバ21および31に送信する(ステップS315)。

【0104】サーバ21および31(図2および図6参照)において、通信部217および317は、伝送路Nからのフォーマット送信要求Dfr1およびDfr2を受信して、ワーキングエリア216および316に転送し格納する(ステップS316)。格納されたフォーマット送信要求Dfr1およびDfr2を解釈した後、中央処理部215および315は、フォーマット格納部218および318に格納されているフォーマットデータDfm1およびDfm2をワーキングエリア216および316に取り出す(ステップS317)。

【0105】中央処理部215および315は、取り出したフォーマットデータDfm1およびDfm2を、ワーキングエリア216および316から通信部217および317に転送し、通信部217および317は、受け取ったフォーマットデータDfm1およびDfm2を、伝送路Nを通じて、交換装置Uc1に送信する(ステップS318)。

【0106】交換装置Uc1(図9参照)において、通信部141は、伝送路NからのフォーマットデータDfm1およびDfm2を受信して、ワーキングエリア13に転送し格納する(ステップS319)。次に、中央処理部12は、フォーマットデータDfm1およびDfm2を参照して、ライセンス情報Dlc1を、ライセンス情報Dlc2に

変換する(ステップS320)。

【0107】ステップS320をより具体的に説明すると、上述の仮定下では、フォーマットデータDfm1およびDfm2を比較することにより、中央処理部12は、利用許可情報Dlw1および利用許可情報Dlw2に使用されるビット数とが相違すると認識する。そのため、中央処理部12は、ライセンス情報Dlc1から利用許可情報Dlw1を取り出して、それを解釈する。その後、中央処理部12は、このような解釈結果に相当する(q2-q1)ビットの利用許可情報Dlw2に、取り出した利用許可情報Dlw1を変換する(ステップS321)。

【0108】さらに、中央処理部12は、今回の変換要求Dcrから、端末識別子1tn2を取り出す(ステップS322)。ここで、注意を要するのは、前述したように、コンテンツ識別子Ict1およびIct2において、コードおよびビット数の双方は同じであり、復号鍵Kd1およびKd2は互いに同じであると仮定されている。それゆえ、中央処理部12は、ライセンス情報Dlc1のコンテンツ識別子Ict1および復号鍵Kd1を、ライセンス情報Dlw2のコンテンツ識別子Ict2および復号鍵Kd2としてそのまま用いる。

【0109】以上の処理により、ワーキングエリア13上には、ライセンス情報Dlc2の構成要素である、端末識別子1tn2、コンテンツ識別子Ict2、利用許可情報Dlw2および復号鍵Kd2が揃う。次に、中央処理部12は、フォーマットデータDfm2に示されるビット位置に従って、これら構成要素を並べて、図15(b)に示すライセンス情報Dlc2を組み立てる(ステップS323)。上述の仮定下では、中央処理部12は、端末識別子1tn2、コンテンツ識別子Ict2、利用許可情報Dlw2および復号鍵Kd2の順番で並べる。

【0110】以上のステップS323までの処理により、ワーキングエリア13上には、ライセンス情報Dlc1から変換されたライセンス情報Dlc2が完成する。次に、中央処理部12は、ワーキングエリア13上のライセンス情報Dlc2を通信部14に転送し、通信部14は、受け取ったライセンス情報Dlc2を、伝送路Nを通じて、端末装置22に送信する(ステップS324)。なお、ライセンス情報Dlc2は、契約者βに無関係な者に利用されてはならないので、交換装置Uc1および端末装置22は、SSL(Secure Socket Layer)に代表される安全な通信下で、ライセンス情報Dlc2を交換することが好ましい。端末装置22(図2参照)において、通信部222は、伝送路Nからのライセンス情報Dlc2を受信する(ステップS325)。

【0111】以上説明したように、本実施形態に係る交換装置Uc1は、契約者βの端末装置22向けのライセンス情報Dlc1を契約者βの端末装置32向けのライセンス情報Dlc2に変換して、当該端末装置22に返す。これにより、契約者βは、自分のライセンス情報Dlc1か

ら変換され、かつ端末装置32側で正しく使えるライセンス情報D1c2を受け取ることができる。契約者 β は、以上のライセンス情報D1c2をオンラインまたはオフラインで、契約者 δ に渡す。ここで、端末装置32は、契約者 δ の操作に従って、受け取ったライセンス情報D1c2内のコンテンツ識別子1c1を含むコンテンツ取得要求をサーバ31に送信する。その結果得られる暗号済みコンテンツデータDc1c2を、端末装置32は、ライセンス情報D1c2を使って復号して利用する。以上の交換装置Uc1を伝送路N上に設置することにより、従来のコンテンツ配信システムが抱えていた問題を解決して、自分のライセンス情報D1c1を、他人に簡単に譲渡することが可能となる。

【0112】また、以上のライセンス情報の交換処理自体は、端末装置22で実行されるのではなく、伝送路N上の交換装置Uc1で実行される。これによって、端末装置22側における、交換処理のための処理負担を軽減することができる。

【0113】なお、以上の第1の実施形態では、ステップS35～S312により、交換装置Uc1は、サーバ21および31との通信により取得した第1の交換可否情報Iack1およびIack2を使って、端末装置22および32が正当なユーザか否かを判定していた。しかし、これに限らず、交換装置Uc1は、サーバ21および31以外から取得した第1の交換可否情報Iack1およびIack2を使って、ステップS312の判定を行っても良いし、予めローカルの補助記憶装置に保持する第1の交換可否情報Iack1およびIack2を使って、ステップS312の判定を行っても良い。

【0114】「第2の実施形態」ところで、前述の第1の実施形態では、互いに同一性のあるコンテンツデータDc1およびDc2は、同じ暗号鍵Kc1およびKc2により暗号化されていた。そのため、端末装置22および32は、互いに同じ復号鍵Kd1およびKd2を使って、暗号化コンテンツデータDc1およびDc2を復号する。しかしながら、事業者 α および γ のポリシーの相違から、コンテンツ配信システムScd1およびScd2の間では、異なる暗号化方式が使用され、その結果、端末装置22および32は互いに異なる復号鍵Kd1およびKd2を使う場合がある。この場合、第1の実施形態に係る交換装置Uc1で交換されたライセンス情報D1c2を使って、暗号済みコンテンツデータDc2を、端末装置32は復号することができるという問題を想定することができる。そこで、第2の実施形態では、このような問題を解決して、コンテンツ配信システムScd1およびScd2の間で異なる暗号化方式が採用されていたとしても、端末装置22のライセンス情報D1c1を、端末装置32が正しく使用できるライセンス情報D1c2に変換する交換装置Uc2を提供することである。

【0115】ここで、交換装置Uc2のブロック構成は、

図9に示す交換装置Uc1の構成と同様である。また、交換装置Uc2の周辺環境は、図1に示すとおりである。そのため、交換装置Uc2において、交換装置Uc1の構成に相当するものには同一の参照符号を付す。ただし、交換装置Uc2のプログラム格納部11には、プログラムPc1ではなく、プログラムPc2が格納される点には注意を要する。

【0116】以下、ライセンス変換時における交換装置Uc2および端末装置22の処理について説明する。端末装置22側では、図17のステップS31およびS32を行って、交換要求Dcrおよびライセンス情報D1c1を、伝送路Nを通じて、交換装置Uc2に送信する。

【0117】交換装置Uc2（図9参照）では、伝送路Nを通じて、交換要求Dcrおよびライセンス情報D1c1が到着すると、プログラムPc2の実行が開始される。より具体的は、中央処理部12は、プログラムPc2に従って、図20および図21に示す処理手順を実行する。図20および図21は、図18と比較すると部分的に同一のステップを有している。そのため、図20および図21において、図18のフローチャートのステップに相当するものには、同一のステップ番号を付して、その説明を簡略化する。

【0118】まず、中央処理部12は、交換要求Dcrおよびライセンス情報D1c1の到着後、図17のステップS312で、端末装置22および32がコンテンツ/配信システムScd1およびScd2の正当なユーザであると判断した後、図20に示すように、交換先特定情報Icl1のみを使って、ステップS314～S315と同様の処理を行って、フォーマット送信要求Dfr1を生成しサーバ21に送信する。その結果、交換装置Uc2のワーキングエリア13には、サーバ21により送信されたフォーマットデータDfm1のみが格納される（ステップS316～S319参照）。

【0119】さらに、中央処理部12は、今回のライセンス情報D1c1からコンテンツ識別子1c1を取り出す（図21；ステップS41）。その後、中央処理部12は、図22に示すように、コンテンツ識別子1c1を含むフォーマット/復号鍵送信要求Dfdを、ワーキングエリア13上で生成する（ステップS42）。ここで、フォーマット/復号鍵送信要求Dfdは、交換先特定情報Icl1で特定されるサーバ31にフォーマットデータDfm2および復号鍵Kd2の送信を要求するための情報である。

【0120】中央処理部12は、生成したフォーマット/復号鍵送信要求Dfdを、ワーキングエリア13から通信部14に転送し、通信部14は、受け取ったフォーマット/復号鍵送信要求Dfdを、伝送路Nを通じて、サーバ31に送信する（ステップS43）。

【0121】サーバ31（図6参照）において、通信部317は、伝送路Nからのフォーマット/復号鍵送信要求Dfdを受信して、ワーキングエリア316に転送し格

納する(ステップS44)。格納されたフォーマット/復号鍵送信要求Dfdを解釈した後、中央処理部315は、まず、フォーマット格納部318に格納されているフォーマットデータDfm2をワーキングエリア316に取り出す(ステップS45)。

【0122】さらに、中央処理部315は、復号鍵DB312の中から、今回のフォーマット/復号鍵送信要求Dfdに含まれるコンテンツ識別子Ict1と同じコードを有するコンテンツ識別子Ict2を検索し、さらに、検索したコンテンツ識別子Ict2と同じ組みの復号鍵Kd2をワーキングエリア324に読み出す(ステップS46)。その後、中央処理部315は、ワーキングエリア316上のフォーマットデータDfm2および復号鍵Kd2を、データセットDst2として、通信部317に転送する。通信部317は、受け取ったデータセットDst2を、伝送路Nを通じて、交換装置Uc2に送信する(ステップS47)。交換装置Uc2(図9参照)において、通信部14は、伝送路NからのデータセットDst2を受信して、ワーキングエリア13に転送し格納する(ステップS48)。

【0123】次に、中央処理部12は、中央処理部12は、フォーマットデータDfm1およびDfm2を参照して、ライセンス情報D1c1を、ライセンス情報D1c2に変換する(ステップS49)。

【0124】ステップS49より具体的に説明すると、まず、中央処理部12は、前述のステップS321を行うことにより、利用許可情報D1w1を利用許可情報D1w2に変換し、さらに、ステップS322を行うことにより端末識別子Int2を取り出す。さらに、中央処理部12は、ステップS48で得られたデータセットDst2から、復号鍵Kd2を取り出す(ステップS410)。また、前述したように、中央処理部12は、ライセンス情報D1c1のコンテンツ識別子Ict1を、ライセンス情報D1w2のコンテンツ識別子Ict2としてそのまま用いる。

【0125】以上の処理により、ワーキングエリア13上には、ライセンス情報D1c2の構成要素である、コンテンツ識別子Ict2、利用許可情報D1w2および復号鍵Kd2が揃う。次に、中央処理部12は、図15(b)に示すライセンス情報D1c2を組み立てる(ステップS411)。ここで、ステップS410およびS411により、ライセンス情報D1c1の復号鍵Kd1は、復号鍵Kd2に変換されることになる。次に、中央処理部12は、ステップS324を実行して、通信部14および伝送路Nを介して、組み立てたライセンス情報D1c2を、端末装置22に送信する。端末装置22(図2参照)において、通信部222は、ステップS325を実行して、伝送路Nからのライセンス情報D1c2を受信する。

【0126】以上説明したように、本実施形態に係る交換装置Uc2は、交換装置Uc1と同様に、端末装置32向

けのライセンス情報D1c2を、端末装置22に返す。特に、交換装置Uc2は、ライセンス情報D1c1のコンテンツ識別子Ict1を使わずに、サーバ32とデータ通信を行って、それに対応するコンテンツ識別子Ict2に付加された復号鍵Kd2を得る。交換装置Uc2は、得られた復号鍵Kd2をライセンス情報D1c2に設定する。これにより、コンテンツ配信システムScd1およびScd2の間で異なる暗号化方式が採用されていたとしても、端末装置22のライセンス情報D1c1を、端末装置32が正しく使用できるライセンス情報D1c2に変換する交換装置Uc2を提供することができる。

【0127】なお、以上の第2の実施形態では、ステップS47およびS48による、交換装置Uc2は、サーバ31との通信により復号鍵Kd2を取得するようにしていた。しかし、これに限らず、交換装置Uc2は、復号鍵Kd2を、サーバ31以外から取得した復号鍵Kd2を使って、ライセンス情報D1c2を作成しても良いし、予めローカルの補助記憶装置に保持する復号鍵Kd2を使って、ライセンス情報D1c2を作成するようにしても良い。

【0128】「第3の実施形態」ところで、従前の実施形態では、交換装置Uc1およびUc2の双方は、端末装置22からの交換要求Dcrに 대응して、ライセンス情報の交換処理を無条件で行っていた。しかしながら、事業者αのポリシーによっては、ライセンス情報の交換処理の対象から除外したい利用条件Cct1がある場合もある。そこで、第3の実施形態では、ライセンス情報の交換処理に制限をかけることが可能な交換装置Uc3を提供することである。

【0129】ここで、交換装置Uc3のブロック構成は、図9に示す交換装置Uc1の構成と同様である。また、交換装置Uc3の周辺環境は、図1に示すとおりである。そのため、交換装置Uc3において、交換装置Uc1の構成に相当するものには同一の参照符号を付す。ただし、交換装置Uc3のプログラム格納部11には、プログラムPc1ではなく、プログラムPc3が格納される点には注意を要する。

【0130】以下、ライセンス交換時における交換装置Uc3および端末装置22の処理について説明する。端末装置22側では、図17のステップS31およびS32を行って、交換要求Dcrおよびライセンス情報D1c1を、伝送路Nを通じて、交換装置Uc3に送信する。ここで、本実施形態において、ライセンス情報D1c1は、図14(b)に示すものと比較すると、図23(a)に示すように第2の変換可否情報1ca1が付加される点で相違する。それ以外に両ライセンス情報D1c1の間に相違点は無いので、図23(a)において、図14(b)に示す情報には同一の参照符号を付け、それぞれの説明を省略する。第2の変換可否情報1ca1は、事業者αのポリシーにより付加され、同じライセンス情報D1c1に含まれる利用許可情報D1w1の交換処理を認めるか否かを

示す情報である。

【0131】次に、図23(b)および同図(c)を参照して、第2の変換可否情報1ca1の具体例を2つ挙げよう。まず、図23(b)において、ライセンス情報Dlc1は、端末識別子1tn1、コンテンツ識別子1ct1、第2の変換可否情報1ca1、複数の利用許可情報Dlw1の一例として利用許可情報Dlw1およびDlw12、ならびに復号鍵Kd1を含んでいる。利用許可情報Dlw1は例えば、再生回数を示しており、利用許可情報Dlw12は例えば、印刷回数を示す。第2の変換可否情報1ca1は、このような全ての利用許可情報Dlw1およびDlw12の変換処理を認めるか否かを示す。また、図23(c)において、ライセンス情報Dlc1は、端末識別子1tn1、コンテンツ識別子1ct1、1つまたは複数の第2の変換可否情報1ca1および利用許可情報Dlw1の組みの一例として、第2の変換可否情報1ca1および利用許可情報Dlw11、第2の変換可否情報1ca12および利用許可情報Dlw12、ならびに復号鍵Kd1を含んでいる。利用許可情報Dlw11およびDlw12は、上述のように、例えば、再生回数および印刷回数を示している。第2の変換可否情報1ca1は、同じ組みの利用許可情報Dlw11の変換処理を認めるか否かを示し、第2の変換可否情報1ca12は、同じ組みの利用許可情報Dlw12の変換処理を認めるか否かを示す。

【0132】変換装置Uc3(図9参照)では、伝送路Nを通じて、端末装置22からの変換要求Derおよびライセンス情報Dlc1が到着すると、プログラムPc3の実行が開始される。より具体的に、中央処理部12は、プログラムPc3に従って、図24に示す処理手順を実行する。図24は、図17と比較すると部分的に同一のステップを有している。そのため、図24において、図17のフローチャートのステップに相当するものには、同一のステップ番号を付して、その説明を簡略化する。

【0133】まず、中央処理部12は、変換要求Derおよびライセンス情報Dlc1の到着後、第2の変換可否情報1ca1をチェックして、全ての利用許可情報Dlw1の変換処理が認められていないか否かを判断する(ステップS51)。全利用許可情報Dlw1の変換処理が認められていなければ、中央処理部12は、今回の受信ライセンス情報Dlc1を端末装置22に送り返し(ステップS52)、図24の処理を終了する。なお、変換装置Uc3は、ステップS51の前に、ステップS35およびS36(図17参照)を行って、サーバ21および31から第1の変換可否情報1ac1および1ac2を取得した後、端末装置22および32がコンテンツ配信システムScd1およびScd2の正当なユーザーかを判定した後に、ステップS51を行っても良い。

【0134】それに対して、ステップS51において、一部または全ての利用許可情報Dlw1の変換処理が認められていないと判断した場合、中央処理部12は、第1の

実施形態で説明したように、変換要求Derおよびライセンス情報Dlc1を格納する(ステップS33)。その後、中央処理部12は、第2の変換可否情報1ca1に従って、全利用許可情報Dlw1の変換が認められているか否かを判断する(ステップS53)。全利用許可情報Dlc1の変換が認められている場合、中央処理部12は、ステップS34からS316(図18参照)までの処理を行う。

【0135】それに対して、ステップS53において、一部の利用許可情報Dlw1の変換処理が認められていると判断した場合、中央処理部12は、第2の変換可否情報1ca1に従って、変換処理が認められている利用許可情報Dlw1と、そうでないものに分類する(ステップS54)。その後、中央処理部12は、変換処理が認められていない利用許可情報Dlw1を端末装置22に送り返し(ステップS55)。その後、変換処理が認められている利用許可情報Dlw1を対象にステップS34からS316(図18参照)までの処理を行う。

【0136】以上の処理により、本実施形態に係る変換装置Uc3は、第2の変換可否情報1ca1を使うことにより、ライセンス情報の変換処理に制限をかけることが可能になる。それによって、事業者αのポリシーを反映可能な変換装置Uc3を実現することが可能になる。

【0137】なお、第3の実施形態において、第2の変換可否情報1ca1はライセンス情報Dlc1に付加されることとして説明した。しかし、第2の変換可否情報1ca1はライセンス情報Dlc1に付加されていないことも良い。この場合、変換装置Uc3は、例えば、変換要求Derおよびライセンス情報Dlc1の到着後、典型的にはサーバ31に、各利用許可情報Dlw1に対応する第2の変換可否情報1ca1を問い合わせ取得し、その後、ステップS51以降の処理を行う。他にも、変換装置Uc3は、コンテンツ配信システムScd1で使われる利用許可情報Dlw1毎に、第2の変換可否情報1ca1を、予めローカルの補助記憶装置に保持しておき、変換要求Derおよびライセンス情報Dlc1の到着後、ローカルの第2の変換可否情報1ca1を使って、ステップS51以降の処理を行っても良い。

【0138】また、第3の実施形態において、中央処理部12は、ステップS54で、変換処理が認められている利用許可情報Dlw1と、そうでないものに分類する。その結果、単一の利用許可情報Dlw1のみがステップS34以降の処理の対象として残ってしまう場合がある。さらに、このような利用許可情報Dlw1が単独では意味をなさないものである場合がある。例えば、利用許可情報Dlw1がコンテンツデータDct1の複製許可を示す場合、変換後のライセンス情報Dlc2を端末装置23が取得したとしても、端末装置22は単に、コンテンツデータDct1の複製が可能とただで、コンテンツデータDct1を再生したり、印刷したりすることができな

い、つまり、このようなライセンス情報D1c2は単独では意味をなさない。このような無意味はライセンス情報の交換処理の実行を遅らせるために、中央処理部12は、ステップS54で選んだ利用許可情報D1w1の内容を検査して、それが有意なものか否かを判断して、意味をなさないものをステップS34以降の処理の対象としないようにすることが好ましい。

【0139】また、第3の実施形態において、中央処理部12は、ステップS52およびS55で、交換処理が認められていない利用許可情報D1w1を端末装置22に送り返すようにしていたが、これに限らず、中央処理部12は、コンテンツ配信システムScd2で、ライセンス情報D1c1に設定される利用許可情報D1w1が利用許可情報として定義されていない場合、交換処理が認められていないと判断して、ステップS55で利用許可情報D1w1を端末装置22に送り返すようにしても良い。なお、このように判断した場合においても、交換装置Uc3は、ローカルまたは遠隔の補助記憶装置で、交換できない利用権情報D1w1を保持しても良いし、サーバ31に返すようにしても良い。

【0140】また、以上の第1〜第3の実施形態では、契約者 β が契約者 α に自分のライセンス情報D1c1を譲渡するために、交換装置Uc1〜Uc3が用いられていた。しかし、交換装置Uc1〜Uc3は、他の状況、例えば、契約者 β が第2のコンテンツ配信システムScd2で利用可能なライセンス情報D1c2を何らかの方法で入手し、入手したライセンス情報D1c2を、自分が加入するコンテンツ配信システムScd1で利用可能なライセンス情報D1c1に変換するような状況にも応用することができる。また、入手したライセンス情報D1c2を、自分が加入しない他のコンテンツ配信システムで利用可能なものに変換する場合にも、交換装置Uc1〜Uc3を応用することができる。

【0141】また、以上の第1〜第3の実施形態では、ステップS314（図18、図21参照）で、交換装置Uc1〜Uc3は、端末装置22に、交換後のライセンス情報D1c2を返していた。しかし、これに限らず、端末装置22は、交換要求Dcrと共に、ライセンス情報D1c2の譲渡先となる端末装置22を一意に特定する情報を、交換装置Uc1〜Uc3に送信する。さらに、交換装置Uc1〜Uc3は、受け取った情報に基づいて、交換後のライセンス情報D1c2を、端末装置22に送信するようにしてもよい。包括的に述べると、交換後のライセンス情報D1c2がどのような方法で端末装置22に渡されてもよい。

【0142】なお、第1の実施形態では、交換装置Uc1がライセンス情報の交換処理を行っていた。しかし、その代わりに、端末装置22に、前述のステップS314からS323までの処理（図18参照）で構成されるプログラムを格納しておいてもよい。また、第2の実施形

態では、交換装置Uc2がライセンス情報の交換処理を行っていた。しかし、その代わりに、端末装置22に、前述のステップS314からS411までの処理（図20および図21参照）で構成されるプログラムを格納しておいてもよい。また、第3の実施形態では、交換装置Uc3がライセンス情報の交換処理を行っていた。しかし、その代わりに、端末装置22に、前述のステップS51（図24参照）以降の処理を行うようにしてもよい。これらによって、端末装置22は、自分自身で、自身向けのライセンス情報D1c1を、端末装置22向けのライセンス情報D1c2に変換することが可能となる。これにより、端末装置22は、交換装置Uc1〜Uc3とデータ通信を行う必要がなくなるため、通信コスト等を減らすことが可能となり、さらに、素早く、端末装置22向けのライセンス情報D1c2を得ることが可能となる。

【0143】また、以上の第1〜第3の実施形態では、交換装置Uc1〜Uc3は、端末装置22に対して発行されるライセンス情報D1c1を、端末装置22で利用できるようなライセンス情報D1c2に変換していた。しかし、これに限らず、交換装置Uc1〜Uc3は、例えば契約者 β に割り当てられた利用権情報Drgt1（図5参照）を交換して、別の契約者 δ のための利用権情報Drgt2を作成してもよい。つまり、ライセンス情報D1c1には、第1〜第3の実施形態で説明したものに限らず、図4に示す利用権情報Drgt1も含まれる。なお、この時の典型的な処理として、交換装置Uc1〜Uc3は、利用権情報Drgt1に設定される契約者 β を特定するための識別子（図5には示さず）を、契約者 δ を特定するための識別子に変換する。

【0144】また、以上の第1〜第3の実施形態では、ライセンス情報の交換処理として、利用許可情報D1w1およびD1w2のビット数の調整を例に挙げて説明したが、これに限らず、例えば、ライセンス情報D1c1およびD1c2は互いに異なる文字セットで生成される場合がある。この場合には、各交換装置Uc1〜Uc3は、サーバ21および31の双方と通信を行って、コンテンツ配信システムScd1およびScd2においてどのような文字セットが使用されているかを確認する。このような確認の結果に基づいて、各交換装置Uc1〜Uc3は、ライセンス情報D1c1の文字セットを、ライセンス情報D1c2のものに変換するようにしてもよい。他にも、交換装置Uc1〜Uc3は、コンテンツ配信システムScd1およびScd2の双方においてどのような文字セットが使用されているかが記述されたテーブルを予め保持している場合には、当該テーブルを参照して、ライセンス情報D1c1の文字セットを、ライセンス情報D1c2のものに変換するようにしてもよい。

【0145】また、ライセンス情報D1c1およびD1c2は、XML(Extensible Markup Language)またはXrML(Extensible rights Markup Language)に代表される

記述言語で記述されていても良い。この場合において、変換装置Uc1~Uc3は、XMLまたはXrMLのタグ値を変換したり、記述言語自体を変換したりして、ライセンス情報D1c1からD1c2への変換処理を行っても良い。

【0146】他にも、ライセンス情報D1c1およびD1c2の構成要素が互いに異なる場合もある。ライセンス情報D1c1には、利用許可情報D1w1があるが、ライセンス情報D1c2には、それに相当する利用許可情報D1w2がない場合が、その典型例である。このような場合にも、変換装置Uc1~Uc3は、サーバ21および31の双方と通信を行って、コンテンツ配信システムScd1およびScd2の双方においてどのような構成要素を使ってライセンス情報D1c1およびD1c2が構成されているかを確認する。このような確認の結果に基づいて、変換装置Uc1~Uc3は、ライセンス情報D1c1の構成要素を、ライセンス情報D1c2のものに合致するように変換処理を行ってもよい。他にも、変換装置Uc1~Uc3は、コンテンツ配信システムScd1およびScd2の双方においてどのような構成要素を使ってライセンス情報D1c1およびD1c2が構成されているかが記述されたテーブルを予め保持している場合には、当該テーブルを参照して、ライセンス情報D1c1の構成要素を、ライセンス情報D1c2のものに合致するように変換処理を行ってもよい。

【0147】他にも、ライセンス情報D1c1およびD1c2の構成要素自体は同じであるが、当該ライセンス情報D1c1およびD1c2における構成要素の配列が互いに異なる場合もある。このような場合にも、各変換装置Uc1~Uc3は、サーバ21および31の双方と通信を行って、コンテンツ配信システムScd1およびScd2の双方においてどのような構成要素の配列でライセンス情報D1c1およびD1c2が構成されているかを確認する。このような確認の結果に基づいて、各変換装置Uc1~Uc3は、ライセンス情報D1c1の構成要素の配列を、ライセンス情報D1c2のものに合致するように変換処理を行ってもよい。他にも、各変換装置Uc1~Uc3は、コンテンツ配信システムScd1およびScd2の双方においてどのような構成要素の配列でライセンス情報D1c1およびD1c2が構成されているかが記述されたテーブルを予め保持している場合には、当該テーブルを参照して、ライセンス情報D1c1の構成要素の配列を、ライセンス情報D1c2のものに合致するように変換処理を行ってもよい。

【0148】また、第1~第3の実施形態では、同一性を有するコンテンツデータDet1およびDet2には、互いに同じコードを有するコンテンツ識別子Ict1およびIct2が割り当てられるとして説明した。しかし、これに限らず、同一性を有するコンテンツデータDet1およびDet2に、コンテンツ配信システムScd1およびScd2において一意なコードを有するコンテンツ識別子Ict1およびIct2が割り当てられてもよい。ただし、この

場合、各変換装置Uc1~Uc3は、ライセンス情報D1c1に含まれるコンテンツ識別子Ict1を、コンテンツ識別子Ict2に変換する必要が生じる。そのため、変換装置Uc1~Uc3は、コンテンツ配信システムScd1およびScd2において互いに同一性を有するコンテンツデータDet1およびDet2に割り当てられるコンテンツ識別子Ict1およびIct2の対応関係が記述されたテーブルを予め保持しておくことが好ましい。変換装置Uc1~Uc3は、このようなテーブルを参照して、ライセンス情報D1c1に含まれるコンテンツ識別子Ict1を、コンテンツ識別子Ict2に変換する。

【0149】また、第1~第3の実施形態では、変換装置Uc1~Uc3は、変換処理の対象となるライセンス情報D1c1を端末装置22から受け取っていた。しかし、これに限らず、変換装置Uc1~Uc3は、サーバ21とデータ通信を行って、端末装置22向けのライセンス情報D1c1を取得しても良い。

【0150】また、第1~第3の実施形態では、サーバ21は、コンテンツデータDet1と、ライセンス情報D1c1とを別々のタイミングで端末装置22に送信するようにしていた。しかし、これに限らず、サーバ21は、ライセンス情報D1c1を電子透かしとして、コンテンツデータDet1に埋め込んで、当該コンテンツデータDet1を端末装置22に同時に送信してもよい。この点については、サーバ31に関しても同様である。

【0151】また、第1~第3の実施形態において、各変換装置Uc1~Uc3は、サーバ21および31からフォーマットデータDfa1およびDfa2を通信により取得するようにしていた(ステップS315~S319)。これにより、各変換装置Uc1~Uc3は、フォーマットデータDfa1およびDfa2を補助記憶装置に常時持っておく必要性がなくなる。しかし、通信による取得に限らず、変換装置Uc1~Uc3は、フォーマットデータDfa1およびDfa2をローカルの補助記憶装置に持ってもよい。これにより、変換装置Uc1~Uc3は、サーバ21および31と通信を行う必要性がなくなるので、ライセンス情報の変換処理を高速に行うことが可能となる。

【0152】また、第1~第3の実施形態において、各変換装置Uc1~Uc3は、ライセンス情報の変換処理の例として、ライセンス情報D1c1のフォーマットをライセンス情報D1c2のものに変換するようにしていた(ステップS320)。より具体的には、利用許可情報D1w1には、利用条件Cct1としての再生回数が1回に設定されており、変換装置Uc1~Uc3は、このような利用許可情報D1w1を、再生回数が1回に設定された利用許可情報D1w2に変換していた。しかし、このようなフォーマット変換に限らず、変換装置Uc1~Uc3は、ライセンス情報D1c1に含まれる利用条件Cct1自体を変換して、異なる利用条件Cct2を含むライセンス情報D1c2を作成するようにしても良い。より具体的に、変換装置U

cl1は、利用条件Cct1 およびCct2の変換比率を使って、ライセンス情報Dcl1の利用条件Cct1を、利用条件Cct2に変更する。これにより、例えば、利用条件Cct1としての再生回数 n_1 が、利用条件Cct2としての再生回数 n_2 に変更される。他の例として、コンテンツデータDct1が静止面を表す場合、利用条件Cct1としての再生回数 n_1 が、利用条件Cct2としての印刷回数 n_2 に変更される。さらに、利用条件Cct1としての有効期間が、利用条件Cct2として利用期間無期限に変更される。また、変換装置Uc1~Uc3は、変換比率を、フォーマットデータDfm1等と同様に外部から取得しても良いし、ローカルに保持していても良い。

【0153】また、以上の第1~第3の実施形態では、プログラムPc1~Pc3は、変換装置Uc1~Uc3に格納されていた。しかし、これに限らず、プログラムPc1~Pc3は、CD-ROMに代表される記録媒体に記録された状態で頒布されても良いし、伝送路Nを通じて配信されても良い。

【0154】また、以上の第1~第3の実施形態において、変換装置Uc1~Uc3、サーバ21および31ならびに端末装置22および32において必要な部分には附タンク技術が実装されていても良い。また、少なくとも利用許可情報Dlm1には、ハッシュに代表される改竄検出に必要な情報が付加されていても良い。

【図面の簡単な説明】

【図1】本発明の第1~第3の実施形態に係る変換装置Uc1~Uc3とそれぞれの周辺環境を示す図である。

【図2】図1のサーバ21および端末装置22の詳細な構成を示すブロック図である。

【図3】同図(a)は、図1の事業者αが準備する暗号済みコンテンツデータect1を説明するための図であり、同図(b)は、図2のコンテンツデータベース211の詳細な構成を示す図である。

【図4】同図(a)および(b)は、図2の復号鍵データベース212およびユーザ情報データベース213の詳細な構成を示す図である。

【図5】図2の利用権データベース214の詳細な構成を示す図である。

【図6】図2のサーバ31および端末装置32の詳細な構成を示すブロック図である。

【図7】同図(a)および(b)は、図6のコンテンツデータベース311および復号鍵データベース312の詳細な構成を示す図である。

【図8】同図(a)および(b)は、図6のユーザ情報データベース313および利用権データベース314の詳細な構成を示す図である。

【図9】図1の変換装置Uc1~Uc3の構成を示すブロック図である。

【図10】図1のコンテンツ配信システムScd1におけるコンテンツ配信時のサーバ21および端末装置22の

処理を示すフローチャートである。

【図11】同図(a)は、図10のステップS11で生成される取得要求Dtrrを示す図であり、同図(b)は、図10のステップS16で読み出されるデータセットDst1を示す図である。

【図12】図1のコンテンツ配信システムScd2におけるライセンス情報提供時のサーバ21および端末装置22の処理を示すフローチャートの前半部分である。

【図13】図1のコンテンツ配信システムScd2におけるライセンス情報提供時のサーバ21および端末装置22の処理を示すフローチャートの後半部分である。

【図14】同図(a)は、図12のステップS22で生成される発行要求Dirを示す図であり、同図(b)は、図13のステップS214で生成されるライセンス情報Dlc1を示す図である。

【図15】同図(a)は、図2のフォーマット格納部218に格納されるフォーマットデータDfm1を示す図であり、同図(b)は、図1のコンテンツ配信システムScd2で利用されるライセンス情報Dlc2を示す図である。

【図16】図6のフォーマット格納部318に格納されるフォーマットデータDfm2を示す図である。

【図17】図9に示す変換装置Uc1および図2の端末装置22のライセンス変換処理時における処理を示すフローチャートの前半部分である。

【図18】図9に示す変換装置Uc1および図2の端末装置22のライセンス変換処理時における処理を示すフローチャートの後半部分である。

【図19】同図(a)は、図17のステップS31で生成される変換要求Dcrを示す図であり、同図(b)および(c)は、図17のステップS35で生成される変換可否要求Dcq1およびDcq2を示す図であり、同図

(d)および(e)は、図17のステップS39で生成される第1の変換可否情報Iack1およびIack2を示す図であり、同図(f)および(g)は、図17のステップS35で生成されるフォーマット送信要求Dfr1およびDfr2を示す図である。

【図20】本発明の第2の実施形態に係る変換装置Uc2が、ライセンス変換処理において、変換要求Dcrを受け取った後に行う処理の前半部分を示すフローチャートである。

【図21】本発明の第2の実施形態に係る変換装置Uc2が、ライセンス変換処理において、変換要求Dcrを受け取った後に行う処理の後半部分を示すフローチャートである。

【図22】図20のステップS42で生成されるフォーマット/復号鍵送信要求Dfdを示す図である。

【図23】同図(a)~(c)は第3の実施形態において変換対象となるライセンス情報Dlc1を示す図である。

【図24】本発明の第3の実施形態に係る変換装置Uc3が、ライセンス変換処理において、変換要求Dcrを受け取った後に行う処理の前半部分を示すフローチャートである。

【符号の説明】

22、32…端末装置

Uc1～Uc3…変換装置

11…プログラム格納部

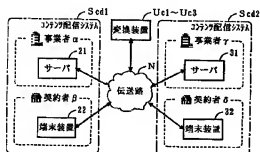
Pc1～Pc3…プログラム

12…中央処理部

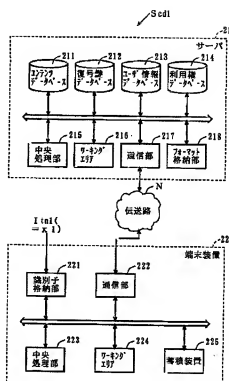
13…ワーキングエリア

14…通信部

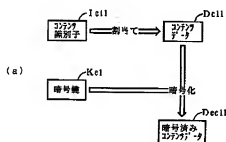
【図1】



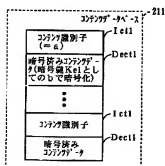
【図2】



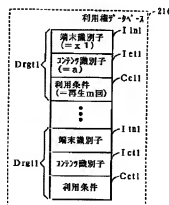
【図3】



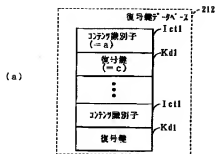
(b)



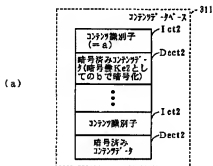
【図5】



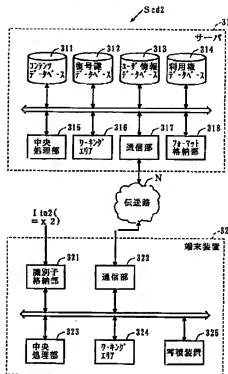
【图4】



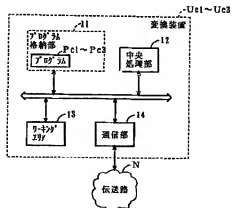
【图7】



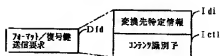
【图6】



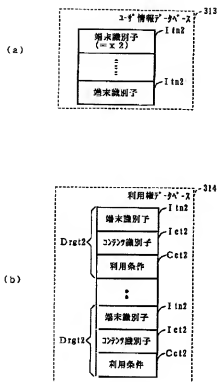
【图9】



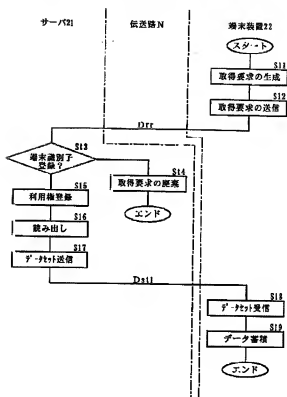
【图22】



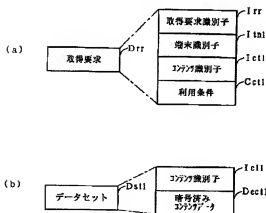
【図8】



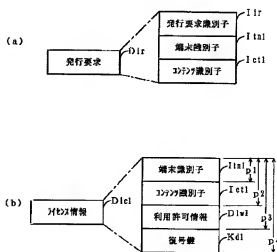
【図10】



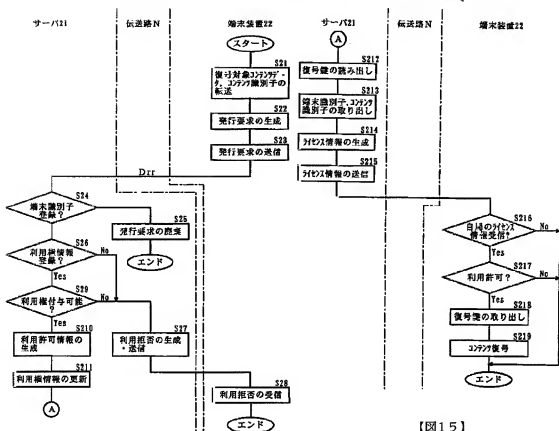
【図11】



【図14】



【图13】



【例 15】

(a)

7x7x7x7 → D1m1

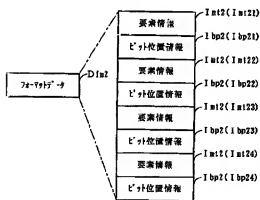
- 要素情報 I m11(I m11)
- 7x7位置情報 I bp1(I bp1)
- 要素情報 I m11(I m12)
- 7x7位置情報 I bp1(I bp2)
- 要素情報 I m11(I m13)
- 7x7位置情報 I bp1(I bp3)
- 要素情報 I m11(I m14)
- 7x7位置情報 I bp1(I bp4)

(b)

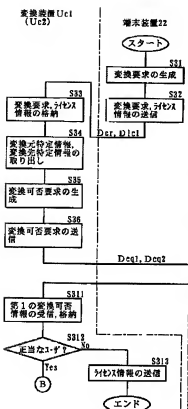
7x7x7x7 → D1c2

- 端末識別子 I tns2
- コンパイル識別子 I c18
- 利用許可情報 D1w2
- 署名鍵 Kd2

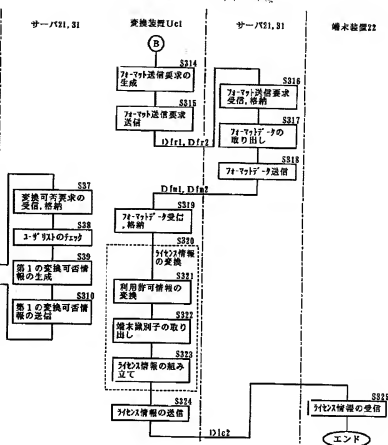
1, 2, 3, 4



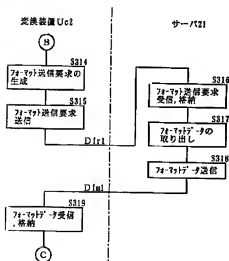
【図17】



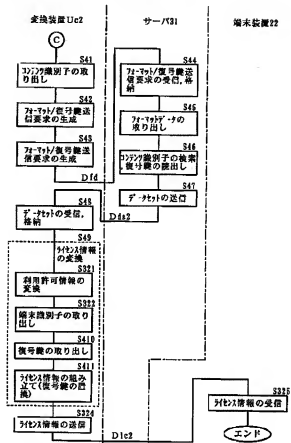
【図18】



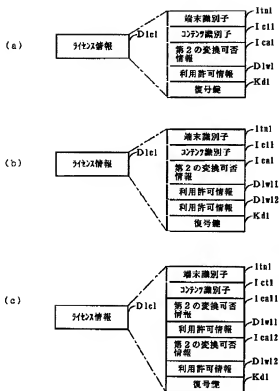
【図20】



【图21】



【図23】



【図24】

